TP-LINK®

网吧专用宽带路由器

TL-R4148

用户手册

1910040127
Rev: 3.0.1

声明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目录

物品清单

请您小心打开包装盒，里面应有以下配件：

- 一台路由器
- 一根串口线
- 一根电源线
- 一本安装手册
- 一张保修卡
- 一张光盘
- 两个用来固定在机架上的 L 型支架及其它配件

⚠ **注意:**

如果发现有配件短缺或损坏的情况，请及时和当地经销商联系。

第1章　　用户手册简介

TL-R4148网吧专用宽带路由器为满足网吧用户需求而设计，除支持普通宽带路由器的功能外，还特别增加针对网吧用户的特色功能，如攻击防护、基于IP的QoS、单机连接数控制、IP与MAC绑定、配置文件下载/导入等。

在您准备安装使用本产品之前，请先仔细阅读本手册，以全面利用本产品的所有功能。

1.1　约定

本手册中所提到的路由器，如无特别说明，系指TL-R4148路由器，下面简称为TL-R4148。

本手册采用的图片中都配有相关参数，实际产品的配置界面并没有提供，请根据实际需要设置这些参数。

本手册中网络拓扑图中所采用的产品图片制作为组网时的参考，与产品实物可能有所差别，请以产品实物图为准。

用户在本用户手册中将会看到几种特殊的图形符号（图标），指出标识中的内容很重要，需要引起您的关注，本用户手册中使用的图标说明如下：

注意: 该图标表示这部分内容很重要，提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。

提示: 该图标为提醒您某些问题出现的可能原因。

举例: 该图标举例说明本设备，具体功能设置的步骤。

1.2　用户手册概述

第 1 章：用户手册简介。

第 2 章：产品概述。简述路由器的功能及主要特性。

第 3 章：硬件安装。帮助您进行路由器的硬件安装。

第 4 章：快速安装指南。帮助您配置路由器的基本网络参数。

第 5 章：配置指南。帮助您配置路由器的高级特性。

附录 A：FAQ。

附录 B：TCP/IP 的详细设置。

附录 C：技术参数表格。

第2章 产品概述

2.1 产品简介

TL-R4148网吧专用宽带路由器为满足网吧用户需求而设计，提供全中文 Web 配置界面，支持在线软件升级功能，满足网吧用户对高性能、多功能、高可靠性、高安全性的需求。

TL-R4148除包含所有宽带路由器常见功能外，还支持攻击防护、基于 IP 的 QoS、单机连接数控制、IP 与 MAC 绑定、端口镜像、配置文件备份/导入等特别适合网吧应用的功能。

攻击防护功能，有效提高网吧的网络可靠性。支持内/外部攻击防范，提供扫描类、DoS 类、可疑包和含有 IP 选项的包等攻击保护，能侦测及阻挡 IP 地址欺骗、源路由攻击、IP/端口扫描、DoS 等网络攻击，有效防止 Nimda、冲击波、木马等病毒攻击，为网吧提供可靠的安全保障。

基于 IP、端口的 QoS，可限制单机带宽、连接数，有效防止用户使用 P2P 等特殊应用过度占用网络资源，让网络游戏更顺畅。可针对网吧划分不同服务区，设置不同的带宽、连接数，保证特殊分区、特殊应用的服务质量，方便网吧分区收费。同时提供连接数列表，详细显示各 IP 当前占用连接数，帮助网吧业主轻松掌握网吧网络资源分配。

支持 IP 与 MAC 绑定，有效防范 ARP 攻击。ARP 攻击在网吧频繁发生，更改路由器 ARP 映射表，使网吧整个网络将陷于瘫痪，影响网吧的正常运营。IP 与 MAC 地址绑定功能，强制 IP 与 MAC 一一对应，不能轻易更改，从而有效防范 ARP 攻击。

支持端口镜像，便于网吧监控。网吧传输的数据可按要求复制到监控端口，满足公安部门的网吧监控要求，也为分析、解决网吧网络问题提供参考数据。

配置备份与导入，可将配置文件保存到电脑，需要复位路由器时，可导入配置文件，缩短配置时间，不影响网吧运营。

2.2 主要特性

- 支持 TCP/IP，DHCP，ICMP，NAT，PPPoE，SNTP，HTTP，DNS 等协议
- 提供 1 个 WAN 口 4 个 LAN 口，10/100Mbps 自适应，支持端口自动翻转（Auto MDI/MDIX）
- 支持基于 IP 或基于端口的 QoS 设置，可限制单机带宽
- 内置简单管理交换机，支持端口带宽控制和端口镜像等功能
- 支持 VPN Pass-through、UPnP 和 DDNS
- 支持 UPnP 和 DDNS
- 支持虚拟服务器、特殊应用程序、DMZ 主机和静态路由等功能
- 支持连接数设置，可限制单机连接数
- 内建防火墙，支持 IP 地址过滤、域名过滤、MAC 地址过滤
- 提供攻击防护，可对网络攻击和病毒攻击进行防范
- 支持 IP 与 MAC 地址绑定，有效防范 ARP 攻击

- 支持 MAC 地址修改和克隆
- 提供系统日志功能，支持外挂 Syslog 服务器记录信息
- 支持 Web 和远程管理，全中文配置界面，支持在线升级
- 支持配置文件备份与载入
- 内置电源，1U 钢壳，可装 19 英寸标准机架，工业级设计

第3章 硬件安装

3.1 面板布置

3.1.1 前面板

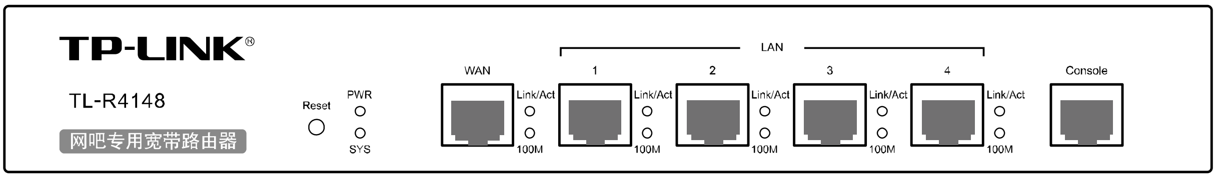


图 3.1 前面板示意图

指示灯：

指示灯	描述	功能
PWR	电源指示灯	常亮表示系统正在运行
SYS	系统指示灯	闪烁表示系统正常
		常亮或不亮表示系统不正常
Link/Act	状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在进行数据传输
100M	速度指示灯	常亮表示相应端口位于 100M 工作模式
		不亮表示相应端口位于 10M 工作模式或未接入设备

- **WAN** 1 个广域网端口(RJ45)。连接 xDSL/Cable Modem 或以太网。
- **局域网端口** 4 个 10/100Mbps 自适应 RJ45 接口，计算机和集线器/交换机通过这个端口连入局域网。
- **Reset** 复位按钮，可以将设备恢复为出厂设置。复位方式：通电状态下长按 RESET 键，待系统指示灯闪烁 5 次后松开 RESET 键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为 http://192.168.1.1，默认用户名和密码均为 admin。

⚠ **注意:**

在路由器未完全启动前，不能关闭电源，否则，配置有可能没有恢复到出厂默认值。

3.1.2 后面板

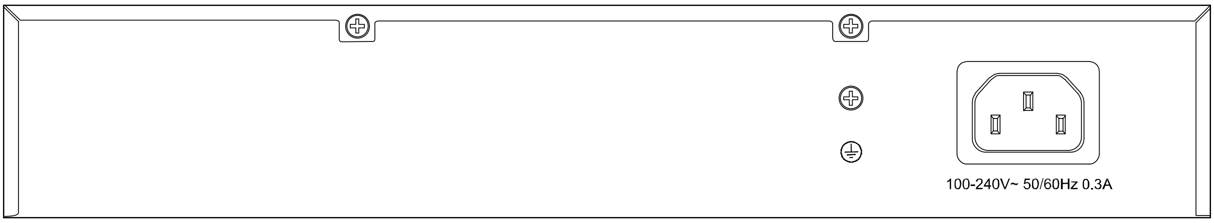


图 3.4 后面板示意图

- **电源插孔** 这个插孔用于插接电源。电源规格为：100-240V~ 50/60Hz 0.3A。如果使用不匹配的电源，可能会导致路由器损坏。

- **防雷接地柱** 位于电源接口左侧，请使用导线接地，以防雷击。详细防雷措施请参见《防雷安装手册》。

3.2 系统需求

- 宽带 Internet 服务（接入方式为 xDSL/Cable Modem 或以太网）
- 具有以太网 RJ45 连接器的调制解调器（直接接入以太网时不需要此物件）
- 每台 PC 的以太网连接（网卡和网线）
- TCP/IP 网络软件（Windows 95/98/ME/NT/2000/XP 自带）
- Internet Explorer 5.0 或更高版本

3.3 安装环境

安装环境要求：

1. 将路由器水平放置。
2. 尽量将路由器放置在远离发热器件处。
3. 不要将路由器置于太脏或潮湿的地方。
4. 电源插座请安装在设备附近便于触及的位置，以方便操作。

路由器推荐使用环境：

- 温度：0 ºC～40 ºC
- 湿度：5％～90％RH，无凝结

3.4 硬件安装步骤

在安装路由器前，请确认是否能通过宽带服务访问网络。如果无法访问，请先和您的网络服务商（ISP）联系解决问题。成功访问网络后，请遵循以下步骤安装您的路由器。安装时拔除电源插头，保持双手干燥。

1) 建立局域网连接

用一根网线连接路由器的 LAN 口和局域网中的集线器或交换机，如下图所示。也可以用一根网线将路由器与计算机网卡直接相连。

2) 建立广域网连接

用网线将路由器 WAN 口与 Internet 相连，如下图所示。

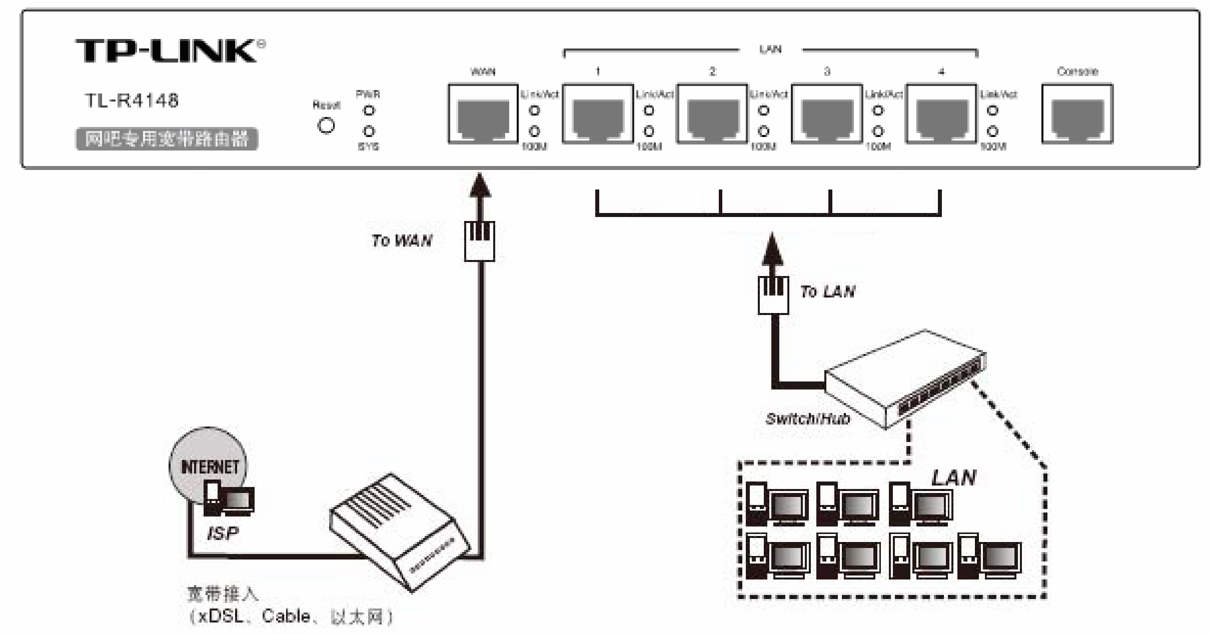


图 3.7 建立局域网和广域网连接

注意:

以上网络拓扑图为您进行网络设置的参照用例，您可以根据实际情况，实际需求配置适合您的网络构架。

3) 连接电源

将电源连接好，路由器将自行启动。

第4章　快速安装指南

如果对路由器进行基本配置，请阅读本章内容；如果进行高级配置，请继续阅读第 5 章内容。

4.1　建立正确的网络设置

路由器默认 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本用户手册上将按默认值说明。

首先请将计算机接到路由器的局域网端口，接下来可以使用两种方法为您的计算机设置 IP 地址。

方法一：手动设置 IP 地址。

设置计算机的 TCP/IP 协议。如果已经正确设置完成，请跳过第一步。

设置计算机的 IP 地址为 192.168.1.xxx（xxx 范围是 2 至 254），子网掩码为 255.255.255.0，默认网关为 192.168.1.1。

方法二：利用路由器内置 DHCP 服务器自动设置 IP 地址。

设置计算机的 TCP/IP 协议为“自动获取 IP 地址”。

在设置好 TCP/IP 协议后，使用 Ping 命令检查计算机和路由器之间是否连通。下面的例子为一个在 Windows XP 环境中，执行 Ping 命令，操作步骤如下：

首先请点击桌面的“开始”菜单，再选择“运行”选项，并在随后出现的运行输入框内输入 cmd 命令，然后回车或点击“确认”键即可进入下图所示界面。

最后在该界面中输入命令 Ping 192.168.1.1，其结果显示如下。

如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

那么计算机已与路由器成功建立连接。如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，请按照下列顺序检查：

1） 硬件连接是否正确？

提示：

路由器面板上对应局域网端口的 Link/Act 指示灯和您计算机上的网卡灯必须亮。

2） 您的计算机的 TCP/IP 设置是否正确？

提示：

如果路由器的 IP 地址为 192.168.1.1，那么您的计算机 IP 地址必须为 192.168.1.xxx（xxx 范围是 2~254）。

4.2 快速安装指南

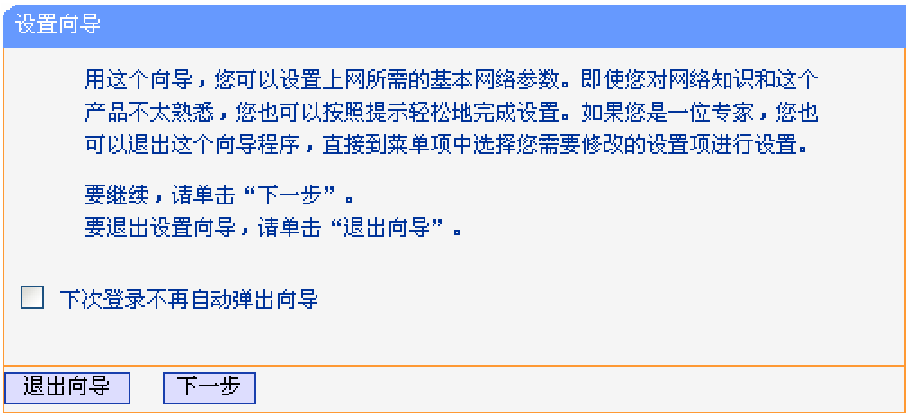
本产品提供基于浏览器（Internet Explorer 或 Netscape Communicator）的配置界面，这种配置方案适宜于任何 MS Windows，Macintosh 或 UNIX 平台。

激活浏览器，取消“使用代理服务器”选项或者将路由器的 IP 地址添加到“代理服务器设置”中的“例外”栏中（在 IE 中选择“工具－Internet 选项－连接－局域网设置”，就可以找到这些设置）。接着在浏览器的地址栏里输入路由器的 IP 地址，例如 http://192.168.1.1。

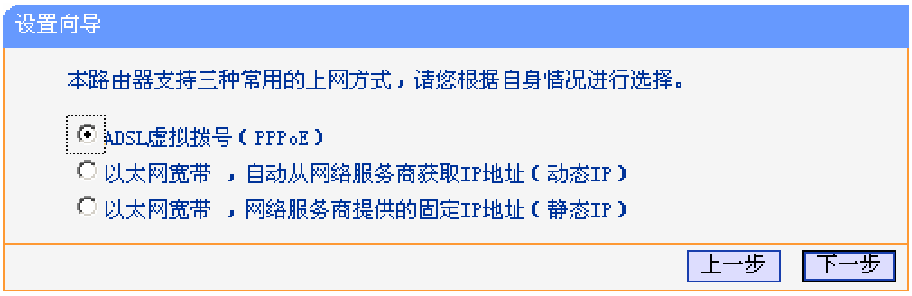
连接建立后将会看到下图所示登录界面。输入用户名和密码（用户名和密码的出厂设置均为“admin”），然后单击确定按钮。



成功登录后会弹出一个设置向导的画面（如果没有自动弹出，可以单击管理员模式画面左边“设置向导”菜单将它激活）。

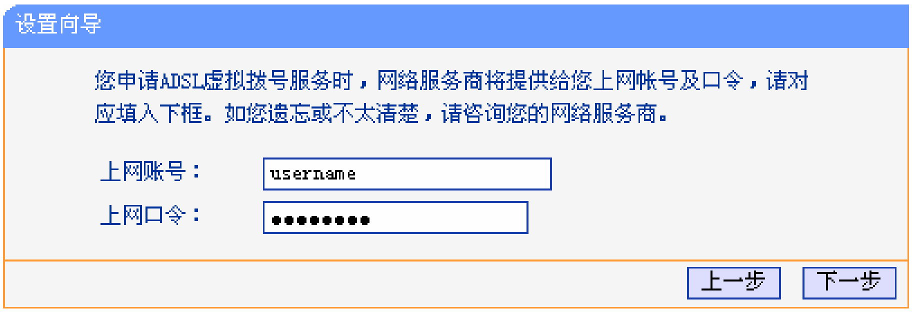


单击“下一步”，进入上网方式选择画面。



以上画面显示了最常用的三种上网方式，可以根据自身情况进行选择，然后单击“下一步”填写上网所需的基本网络参数。

1) 如果您的上网方式为 PPPoE，即 ADSL 虚拟拨号方式，则需要填写以下内容：



- **上网帐号**　　填入 ISP 为您指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- **上网口令**　　填入 ISP 为您指定的 ADSL 上网口令，不清楚可以向 ISP 询问。

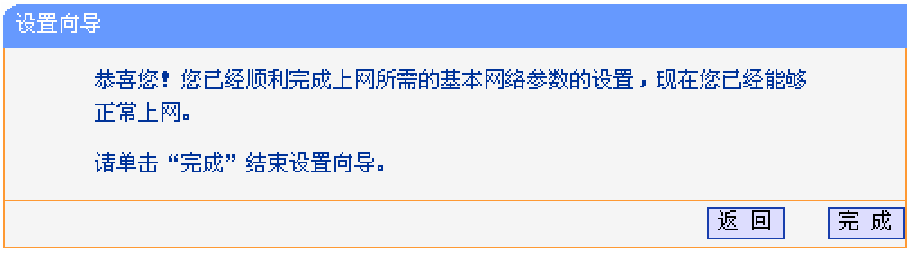
2) 如果您的上网方式为动态 IP，即可以自动从网络服务商获取 IP 地址，则不需要填写任何内容即可直接上网。

3) 如果您的上网方式为静态 IP，即拥有网络服务商提供的固定 IP 地址，则需要填写以下内容：



- **IP 地址**　　本路由器对广域网的 IP 地址，即 ISP 提供给您的 IP 地址，不清楚可以向 ISP 询问。
- 子网掩码　　本路由器对广域网的子网掩码，即 ISP 提供给您的子网掩码，一般为 255.255.255.0。
- 网关　　填入 ISP 提供给您的网关，不清楚可以向 ISP 询问。
- **DNS 服务器**　　填入 ISP 提供给您的 DNS 服务器地址，不清楚可以向 ISP 询问。
- **备用 DNS 服务器**　　可选项，如果 ISP 提供给您了两个 DNS 服务器地址，则您可以 把另一个 DNS 服务器地址的 IP 地址填于此处。

在填写完上网所需的基本网络参数之后，会出现设置向导完成界面。



第5章　配置指南

5.1　启动和登录

在启动和登录成功以后，浏览器会显示管理员模式下的路由器配置页面。

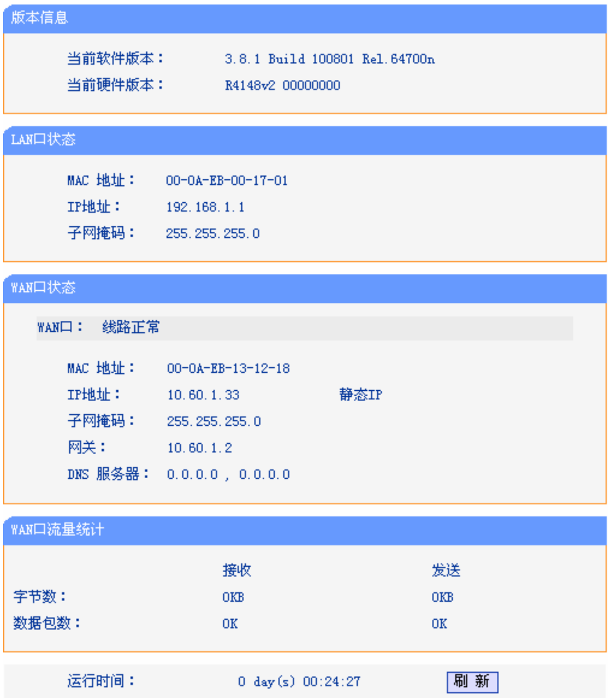


在左侧菜单栏中，共有“运行状态”、“设置向导”、“网络参数”、“DHCP 服务器”、“转发规则”、“安全设置”、“路由功能”、“连接数限制”、“QoS”、“IP 与 MAC 绑定”、“花生壳 DDNS”、“交换机功能”和“系统工具”十三个菜单。单击某个菜单项，您即可进行相应的功能设置。

在使用过程中，如果您对本产品的功能有任何疑问，您只需单击该页面的“帮助”按钮，即可获得详细的联机帮助。

下面将详细讲解各个菜单的功能。

5.2　运行状态



本页显示路由器的工作状态。

- **版本信息** 此处显示当前的软、硬件版本。
- **LAN 口状态** 此处显示当前 LAN 口的 MAC 地址、IP 地址和子网掩码。
- **WAN 口状态** 此处显示当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器。同时 IP 地址右侧将显示用户上网方式（PPPoE/动态 IP/静态 IP）。如果用户的上网方式为 PPPoE（ADSL 拨号上网）的话，当用户已经连接上 Internet 时，此处将会显示用户的上网时间和“断线”按钮，单击此按钮可以进行即时的断线操作，当用户未连接 Internet 时，此处将会显示“连接”按钮，单击此按钮可以进行即时的连接操作。
- **WAN 口流量统计** 此处显示当前 WAN 口接收和发送的数据流量信息。

5.3 设置向导

请参考第 4 章的快速安装指南。

5.4 网络参数



在“网络参数”菜单下面，共有“LAN 口设置”、“WAN 口设置”、“MAC 地址克隆”、和“WAN 端口参数”四个子项。单击其中某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.4.1 LAN口设置

选择网络参数下的 LAN 口设置项，将进入 LAN 口的设置界面，如下图示。请按照下面各子项说明设置该 LAN 口的参数。



- **MAC 地址** 设置路由器对局域网的 MAC 地址。
- **IP 地址** 请输入本路由器对局域网的 IP 地址。该 IP 地址出厂默认值为 192.168.1.1，请根据实际需要设置该值。

➢ **子网掩码**　　本路由器对局域网的子网掩码，可以在下拉列表中选择 B 类（255.255.0.0）或者 C 类（255.255.255.0）地址的子网掩码。一般情况下选择 255.255.255.0 即可。

注意：

如果您改变了此处 LAN 口的 IP 地址，则您必须用新的 IP 地址才能登录路由器管理界面，并且局域网中所有计算机的默认网关也必须设置为该 IP 地址，这样才能正常上网。

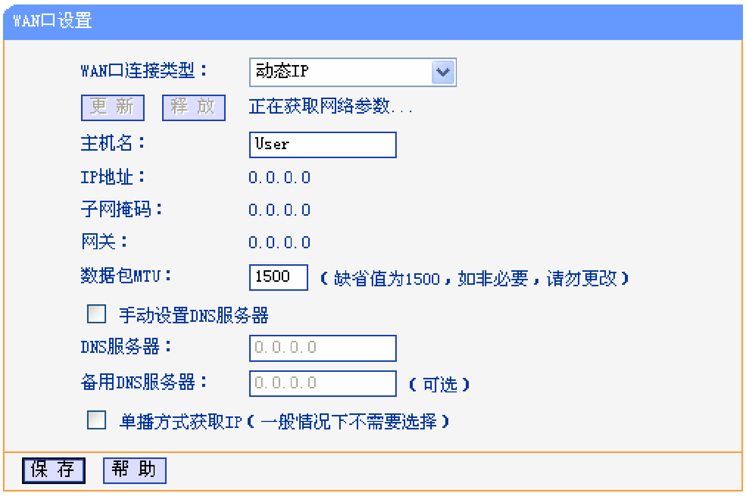
局域网中所有计算机的子网掩码必须与此处子网掩码相同。

5.4.2　WAN口设置

选择网络参数下的 WAN 口设置项，将进入 WAN 口的设置界面（默认为动态 IP 设置界面），如下图示。首先请选择 WAN 口的连接类型，即上网方式。本路由器默认上网方式为“动态 IP”。

5.4.2.1 动态IP

如果选择的 WAN 口连接类型是“动态 IP”，即可以从网络服务商（ISP）自动获取 IP 地址，其设置界面如下图示。请按照下面各子项说明，设置相应的参数。



➢ **WAN 口连接类型**　　上图中选择的是“动态 IP”上网方式。本路由器支持三种常用的上网方式：动态 IP、静态 IP、PPPoE 方式，请根据实际情况选择。

➢ **IP 地址**　　显示从 ISP 的 DHCP 服务器动态得到的 IP 地址，它是路由器对广域网的地址。

➢ 子网掩码　　显示从 ISP 的 DHCP 服务器动态得到的子网掩码。

➢ 网关　　显示从 ISP 的 DHCP 服务器动态得到的网关。

➢ 数据包 **MTU**　　请输入需要限制的数据包的最大长度（MTU），可以输入的范围是 576～1500，默认值为 1500。若非必要，请不要修改该默认值。

➢ 手动设置 **DNS** 服务器　　选择该复选框，可以手动设置自己想要的 DNS 服务器地址。

➢ **DNS** 服务器　　显示从 ISP 的 DHCP 服务器动态得到的 DNS 服务器地址，也可以在此处手动设置想要的 DNS 服务器地址。

- **备用 DNS 服务器**　　显示从 ISP 的 DHCP 服务器动态得到的备用 DNS 服务器地址，也可以在此手动设置想要的备用 DNS 服务器地址，可以不选。
- **单播方式获取 IP**　　如果的 ISP 服务器支持以单播方式获取 IP 地址，请选择该复选框，将以单播的方式从 ISP 获取 IP 地址。

注意:

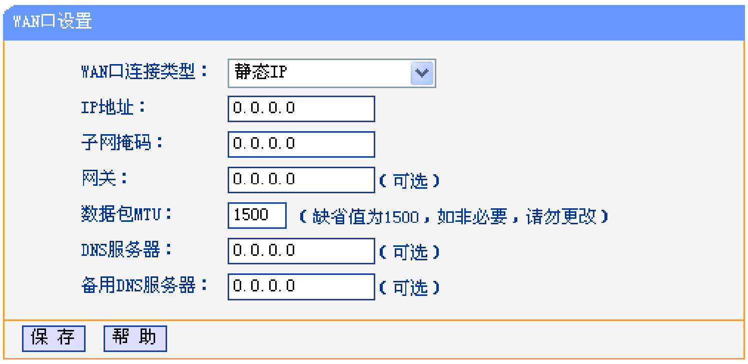
单播方式获取 IP 是指主机以点对点的单播包向指定的 DHCP 服务器请求分配 IP 地址。大多数网络服务商的 DHCP 服务器支持广播的请求方式，只有少数是支持单播的请求方式。如果您在网络连接正常的情况下无法获取 IP 地址，可以选择单播的方式（一般情况下不要选择此项）。

- **按钮功能**　　包括“更新”和“释放”按钮。
- 更新　　单击此按钮，可以从 ISP 的 DHCP 服务器更新 WAN 口的 IP 地址、子网掩码、网关、DNS 服务器等设置。
- 释放　　单击此按钮，本路由器将发送 DHCP 释放操作到 ISP 的 DHCP 服务器，释放 IP 设置。

设置完上面的参数后，点击保存按钮，设置的参数将生效。

5.4.2.2 静态IP

如果选择的 WAN 口连接类型是“**静态 IP**”，即拥有网络服务商（ISP）提供的固定 IP 地址，其设置界面如下图示。请按照下面各子项说明设置相应的参数。

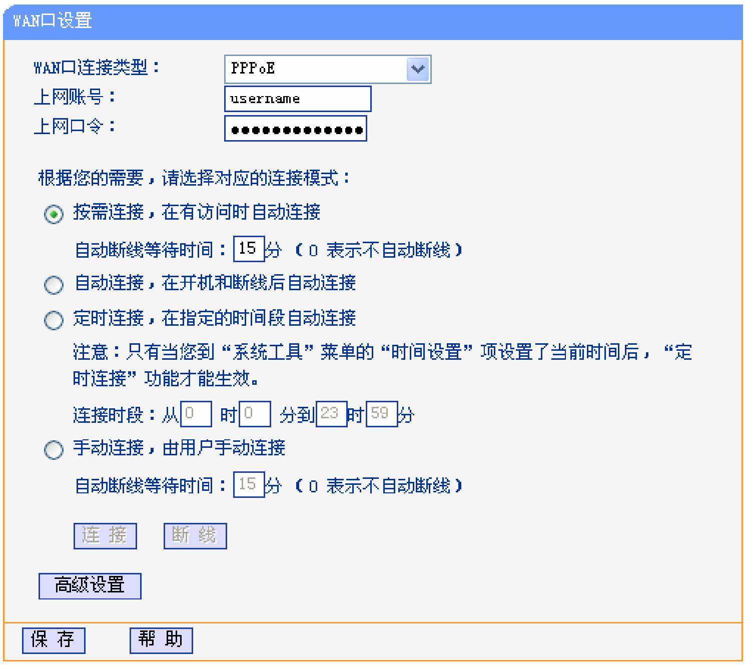


- **IP 地址**　　请输入 ISP 提供的固定 IP 地址，它是路由器对广域网的 IP 地址，不清楚可以向 ISP 询问。
- **子网掩码**　　请输入 ISP 提供的子网掩码，它是路由器对广域网的子网掩码，一般为 255.255.255.0。
- **网关**　　请输入 ISP 提供的网关，不清楚可以向 ISP 询问。
- **数据包 MTU**　　请输入需要限制的数据包的最大长度（MTU），可以输入的范围是 576～1500，默认值为 1500。若非必要，请不要修改该默认值。
- **DNS 服务器**　　请输入 ISP 提供的一个 DNS 服务器地址，不清楚可以向 ISP 询问，也可以不填。

- **备用 DNS 服务器**　请输入 ISP 提供的另一个 DNS 服务器地址，也可以不填。

5.4.2.3 PPPoE

如果选择的 WAN 口连接类型是“**PPPoE**”，即可以从网络服务商（ISP）自动获取 IP 地址时，其设置界面如下图示。请按照下面各子项说明设置相应的参数。



- **上网帐号**　请输入 ISP 指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- **上网口令**　请输入 ISP 指定的 ADSL 上网口令，不清楚可以向 ISP 询问。
- **按需连接**　选中该复选框，则表示将采用按需连接模式，即当有局域网的网络访问请求时，系统将自动连接网络。
- 自动断线等待时间　若选择上面的按需连接模式，则还需在此输入自动断线等待时间（T）。如果 T 不等于 0，则在检测到连续 T 分钟内，若没有网络访问流量系统则会自动断开网络连接，节省您的上网资源。若 T 等于 0，则表示系统不会自动断线。
- **自动连接**　选中该复选框，则表示将采用自动连接模式，即在开机后系统会自动进行连接操作。在使用过程中，如果由于外部原因，网络被断开，则系统会每隔一段时间（30 秒）尝试进行连接，直到连接成功为止。
- **定时连接**　选中该复选框，则表示将采用定时连接模式，即系统在“连接时段”指定的起始时间进行连接操作，在指定的终止时间自动进行断线操作。
- **连接时段**　若选择上面的定时连接，则还需在此设置连接时段，即定时连接的起始和终止时间。
- **手动连接**　选中该复选框，则表示将采用手动连接模式，即在需要连接网络时，自己手动进行 ADSL 拨号连接。与此同时，还需在此输入自动断线等待时间（T）。具体设置同上面所述。
- **按钮功能**　包括“连接”和“断线”两个按钮。

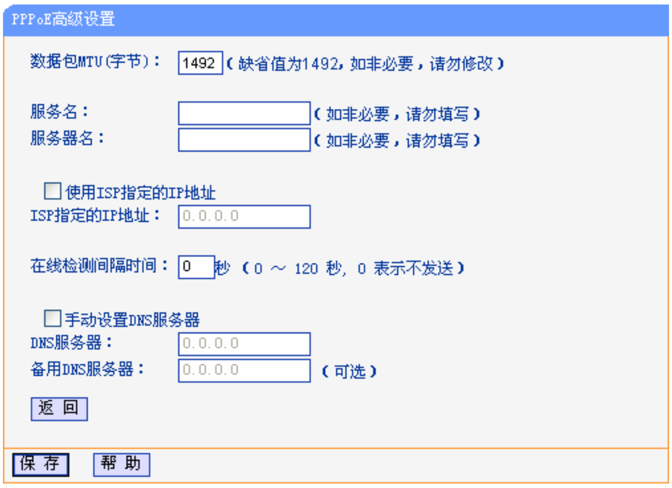
- 连接　　单击此按钮，进行即时的连接操作。
- 断线　　单击此按钮，进行即时的断开操作。

注意:

只有当您在“系统工具”的“时间设置”项，设置了当前时间后，“定时连接”功能才能生效。

您可以根据需要选择上面 4 种连接方式中的任意一种，设置完后可以点击保存按钮，使设置生效。

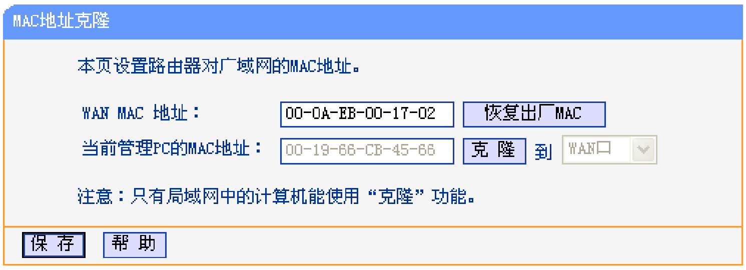
您还可以根据实际需要，进入到“高级设置”界面对相关设置项进行设置、调整。其设置界面如下图示，您可以按照下面各子项说明设置相应的参数。



- **数据包 MTU**　　请输入需要限制的数据包的最大长度（MTU），默认值为 1492。若非必要，请不要修改该默认值。
- **服务名**　　Service Name，若不是 ISP 特别要求，请不要填写。
- **服务器名**　　AC Name，如果不是 ISP 特别要求，请不要填写。
- **使用 ISP 指定的 IP 地址**　　选中复选框，可以设置 ISP 提供的指定 IP 地址。
- **ISP 指定的 IP 地址**　　请输入 ISP 提供的指定 IP 地址。
- **在线检测时间间隔**　　请根据需要填写所需的在线检测时间间隔。路由器将根据该时间间隔发送检测信号，以检测服务器是否在线。若该值为 0，则表示不发送检测信号。如果在系统日志中经常发现有“接收 PADT,服务端请求断开本次连接”这样的日志信息时，请将该值设为 0。
- **DNS 服务器**　　请输入 ISP 提供的一个 DNS 服务器地址，不清楚可以向 ISP 询问，也可以不填。
- **备用 DNS 服务器**　　请输入 ISP 提供的另一个 DNS 服务器地址，也可以不填。

5.4.3　MAC地址克隆

选择网络参数下的 MAC 地址克隆项，将进入下面的设置界面，如下图示。请按照下面各子项说明正确使用该功能。



- **MAC 地址**　　显示当前路由器对广域网的 MAC 地址，此值一般不用更改。但某些 ISP 可能要求对 MAC 地址进行绑定，此时 ISP 会提供一个有效的 MAC 地址给用户，您只要根据它所提供的值，输入到“MAC 地址”栏，然后单击“保存”，即可根据 ISP 的要求更改本路由器对广域网的 MAC 地址。
- **恢复出厂 MAC**　　若您要恢复本路由器对广域网的出厂默认 MAC 地址，则您可以单击此按钮来恢复。
- **当前管理 PC 的 MAC 地址**　　显示当前正在进行管理操作的计算机的 MAC 地址。
- **克隆**　　单击此按钮，您即可把当前管理 PC 的 MAC 地址克隆到 WAN 口。

注意:

只有局域网中的计算机能使用“克隆 MAC 地址”功能。

5.4.4　WAN端口参数

选择网络参数下的 WAN 端口参数，将进入下面的设置界面。该页面提供端口状态、端口流量控制、端口速率等设置。请按照下面各子项说明正确设置这些参数。



- **端口状态表**　　该项用来设置并显示 WAN 端口的状态信息。
- 端口状态　　请根据需要设置 WAN 口的状态，启用或禁用。

- 流量控制　　请根据需要启用或禁用流控模式。启用表示对该端口的数据流量进行控制，反之则不加控制。
- 协商模式　　请根据需要选择协商模式：自协商、10M 半双工、10M 全双工、100M 半双工或 100M 全双工模式。
- **协商状态表**　　该项用来显示端口的协商状态信息。
- 端口状态　　显示端口连接状态，即是否已经连接上。
- 连接速率　　显示端口连接采用的速率。
- 双工模式　　显示端口通信采用的双工模式，全双工或半双工。
- 流量控制　　显示端口是否启用了流量控制。
- **端口限制信息表**　　该项用来设置并显示端口的各种限制信息。
- 入口限制模式　　该项用来选择对进入该 WAN 口的数据包采用的限制类型：所有帧、广播和多播、广播或不限制。
- 入口限制速率　　该项用来限制进入该 WAN 口的数据包速率，其中可选项有 128Kbps、256Kbps、512Kbps、1Mbps、2 Mbps、4 Mbps、8Mbps。
- 出口限制　　选中该复选框表示启用出口限制，即对该 WAN 口转发的数据包进行限制，不选中该复选框则表示不启用出口限制。
- 出口限制速率　　该项用来限制从该 WAN 口转发的数据包速率，其中可选项有 128Kbps、256Kbps、512Kbps、1Mbps、2Mbps、4Mbps、8Mbps。

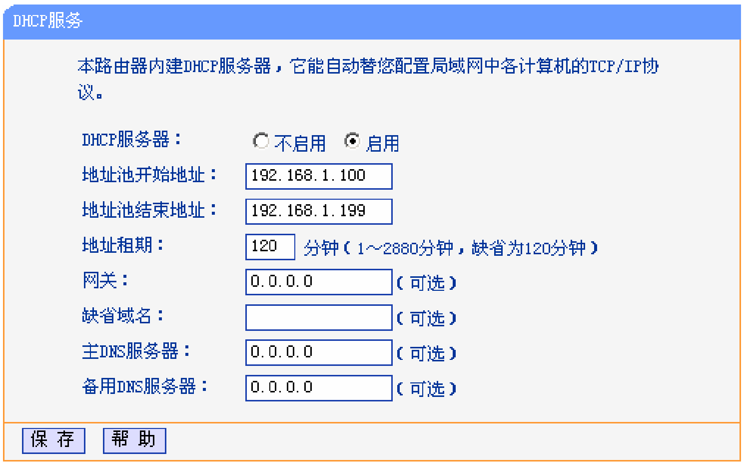
5.5 DHCP服务器



DHCP 服务器主要用来自动配置和管理网络内部主机的 TCP/IP 参数。在“DHCP 服务器”菜单下面，有“DHCP 服务”、“客户端列表”和“静态地址分配”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.5.1 DHCP服务

选择 DHCP 服务器下的 DHCP 服务，将进入下面的设置界面。使用本路由器的 DHCP 服务器功能可以让 DHCP 服务器自动配置局域网中各计算机的 TCP/IP 协议。请按照下面各子项说明正确设置这些参数。



- **DHCP 服务器**　　若想使用 DHCP 的自动配置 TCP/IP 参数功能，请选择启用。
- **地址池开始地址**　　请输入 DHCP 服务器自动分配 IP 地址的起始地址。
- **地址池结束地址**　　请输入 DHCP 服务器自动分配 IP 地址的结束地址。
- **地址租期**　　请输入所分配 IP 地址的有效使用时间，超时将重新分配。
- **网关**　　请输入路由器 LAN 口的 IP 地址，本路由器缺省是 192.168.1.1。
- **缺省域名**　　请输入本地网域名，也可以不填。
- **主 DNS 服务器**　　请输入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问，也可以不填。
- **备用 DNS 服务器**　　如果 ISP 提供了两个 DNS 服务器地址，则请输入另一个 DNS 服务器的 IP 地址，也可以不填。

注意:

为了使用本路由器的 DHCP 服务器功能，局域网中计算机的 TCP/IP 协议必须设置为“自动获得 IP 地址”。

5.5.2　　客户端列表

选择 DHCP 服务器下的客户端列表，将进入下面界面。该客户端列表罗列了所有通过 DHCP 获得 IP 的主机信息，具体如下图示：



- **ID**　　条目序号。
- **客户端名**　　显示分配到 IP 地址的客户端的计算机名。
- **MAC 地址**　　显示分配到 IP 地址的客户端的计算机的 MAC 地址。

- **IP 地址**　　显示 DHCP 服务器分配给客户端的计算机的 IP 地址。
- **有效时间**　　显示主机通过 DHCP 获得 IP 地址后，该 IP 地址剩余的有效时间。客户端软件会在租期到期前自动续约。

5.5.3 静态地址分配

选择 DHCP 服务器下的静态地址分配，将进入下面的设置界面。为了方便您对局域网中计算机的 IP 地址进行控制，本路由器内置了静态地址分配功能。它可以为指定 MAC 地址的计算机预留静态 IP 地址。之后，若此计算机请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动给它分配此预留的 IP 地址。具体设置见下图示：



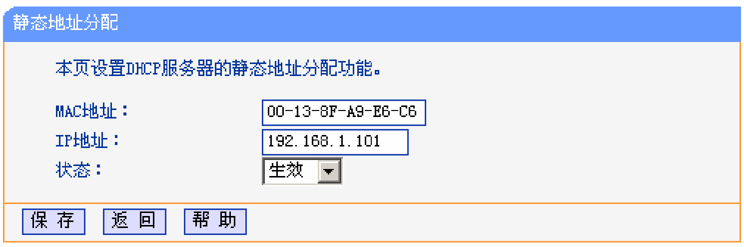
- **静态地址条目表**　　显示静态地址条目信息。
- MAC 地址　　显示预留了 IP 地址的计算机的 MAC 地址。
- IP 地址　　显示预留的 IP 地址
- 状态　　显示该条目是否生效。
- 配置　　显示对该条目进行的超级链接——编辑或删除。
- **添加新条目**　　单击该按钮，可以增加新的静态地址条目，详见后面所述。
- **使所有条目生效**　　单机该按钮，可以使所有静态条目生效。
- **使所有条目失效**　　单机该按钮，可以使所有静态条目失效。
- **删除所有条目**　　单机该按钮，可以删除当前列表中的所有启用或未启用的静态条目。

⚠ **注意：**

此功能需要在重启路由器后才能生效。

5.5.3.1 添加或编辑静态地址

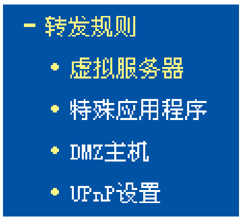
点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面。该页用来设置静态地址条目。



- **MAC 地址** 请输入预留了 IP 地址的计算机的 MAC 地址。
- **IP 地址** 请输入要预留的 IP 地址。
- **状态** 请选择该条目是否生效。

设置完以上三项后，点击保存按钮，该设置将会在静态地址条目表中显示。

5.6 转发规则



在“转发规则”菜单下面，有“虚拟服务器”、“特殊应用程序”、“DMZ 主机”和“UPnP 设置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.6.1 虚拟服务器

选择转发规则下的虚拟服务器，您将进入下面的设置界面。本路由器自身集成了防火墙功能，在路由器默认设置下，广域网中的计算机不能通过本路由器访问局域网中的某些服务器。但是，为了让路由器既保护局域网内部不被侵袭，又方便广域网中合法的用户访问，路由器提供了虚拟服务器功能。虚拟服务器可以定义一个服务端口，外网所有对此端口的服务请求都将被重新定位给路由器指定的局域网中的服务器（通过 IP 地址指定），这样外网的用户便能成功访问局域网中的服务器，而不影响局域网内部的网络安全。具体设置界面如下图示。

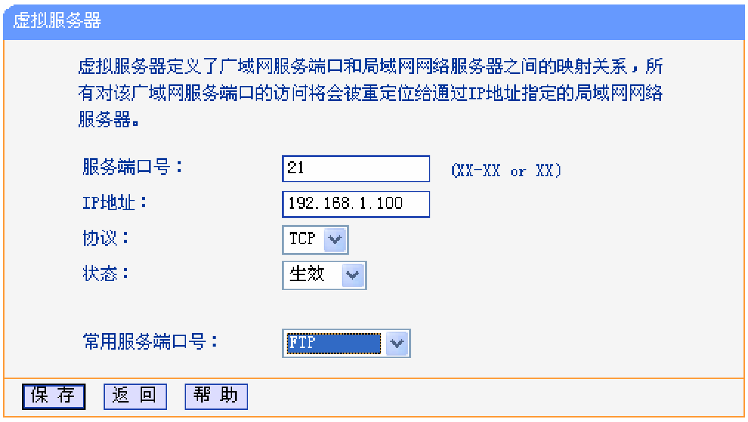


- **虚拟服务器条目表** 显示虚拟服务器条目信息。
- 服务端口 显示 WAN 端服务端口，即路由器提供给广域网的服务端口，外网对该端口的访问都将重定位到局域网中指定的服务器。
- IP 地址 显示局域网中指定为服务器的计算机的 IP 地址。外网对该局域网的访问都将重定位到该指定的计算机。
- 协议 显示数据包的协议类型。
- 状态 显示条目的状态。只有生效时，该条目的设置才起作用。
- 配置 显示对该条目操作的超级链接——编辑或删除。

- 添加新条目　　点击该按钮，可以添加新的虚拟服务器条目。
- 使所有条目生效　　点击该按钮，可以使所有虚拟服务器条目生效。
- 使所有条目失效　　点击该按钮，可以使所有虚拟服务器条目失效。
- 删除所有条目　　点击该按钮，可以删除所有已设的虚拟服务器条目。

5.6.1.1 添加或编辑虚拟服务器

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面。下面以添加新的虚拟服务器条目为例。



- 服务端口号　　请输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，中间用“-”隔开。如上界面所示。
- 常用服务端口号　　请在该项选择服务端口号。在“常用服务端口”中，列出了常用协议的端口，可以直接从其中选择一个，系统会直接将选中的端口填入服务端口号中。对于常用服务端口中没有列出的端口，也可以在服务端口号处手动输入。

设置完成后，请点击保存按钮，然后在局域网服务器上进行相应的设置，这样，广域网中的计算机便可以成功访问局域网中的服务器了。

举例:

如果您的FTP服务器（端口号为21）IP地址为192.168.1.2，Web服务器（端口号为80）地址为192.168.1.3，POP3服务器（端口号为110）IP地址为192.168.1.6，这时您需要指定如下的虚拟服务器映射表：



注意:

如果设置了服务端口为 80 的虚拟服务器，则需要将“系统工具”菜单中的“远端 WEB 管理”项的 WEB 管理端口设置为 80 以外的值，如 8080。否则会发生冲突，从而导致虚拟服务器设置无效。

5.6.2 特殊应用程序

选择转发规则下的特殊应用程序，将进入下面的设置界面。某些程序需要多条连接，如 Internet 网络游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的 NAT 路由器下工作。然而，特殊应用程序使得某些这样的应用程序能够在 NAT 路由器下工作。当一个应用程序给触发端口上发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。



- **虚拟服务器条目表**　　显示虚拟服务器条目信息。
- 触发端口　　显示应用程序首先发起连接的端口，即触发端口。

注意:

触发端口是为应用程序申请建立连接时，路由器指定的用于触发应用程序的端口。只有给该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。

- 触发协议　　显示触发端口上使用的协议，选项有 ALL、UDP 和 TCP。
- 开放端口　　显示该特殊应用程序条目采用的开放端口。

注意:

开放端口是为应用程序提供服务的多个端口。当给触发端口上发起连接后，开放端口打开，之后应用程序便可以给这些开放端口上发起后续的连接。

- 开放协议　　显示开放端口采用的协议，选项有 ALL、UDP 和 TCP。
- 状态　　显示该条目状态，只有状态为生效时，本条目所设的规则才能生效。
- 配置　　显示对该条目的超级链接——编辑或删除。
- **添加新条目**　　点击该按钮，可以在列表中添加新的条目，详见下面章节所述。

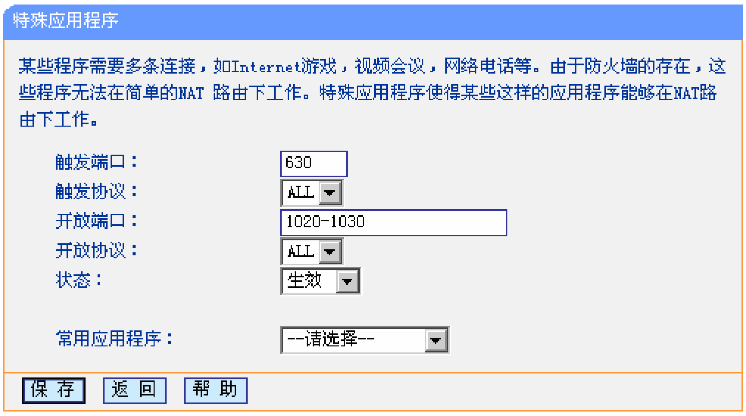
➢ **使所有条目生效** 点击该按钮，可以将该列表中的所有条目的状态设为“生效”。

➢ **使所有条目失效** 点击该按钮，可以将该列表中的所有条目的状态设为“失效”。

➢ **删除所有条目** 点击该按钮，可以删除当前已设的所有条目。

5.6.2.1 添加或编辑特殊应用程序

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面。



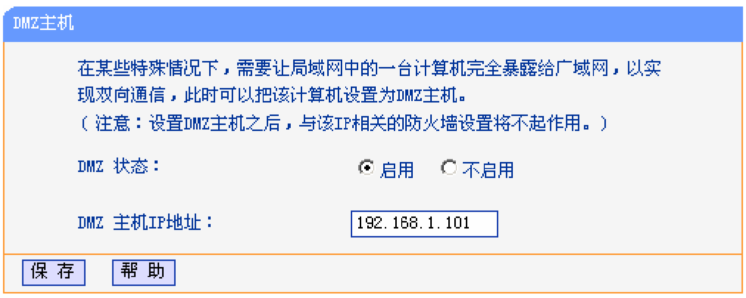
➢ **触发端口** 请输入应用程序首先发起连接的端口触发号，如上图示。

➢ **开放端口** 请输入为应用程序提供服务的开发端口号，如上图示。可以输入一个或者多个端口或端口段，端口段输入格式为“开始端口-结束端口”，中间用“-”隔开，不同的端口段用“,”隔开。

➢ **常用应用程序** 请在该项选择应用程序。在“常用应用程序”中，列出了常用的应用程序，可以直接在其中选中一个，系统会直接将选中的应用程序的触发端口和开发端口号自动填入到对应项中。对于“常用应用程序”中没有列出的端口，也可以在触发端口和开放端口处手动输入。

5.6.3 DMZ主机

选择转发规则下的 DMZ 主机，将进入下面的设置界面。在某些特殊情况下，我们需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为 DMZ 主机。设置界面如下。



、

➢ **DMZ 主机 IP 地址** 请您输入局域网中指定为 DMZ 主机的 IP 地址。

举例：

DMZ 主机设置步骤如下：

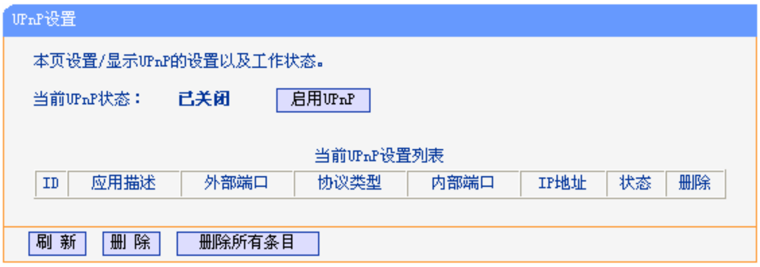
首先在 DMZ 主机 IP 地址栏内输入欲设为 DMZ 主机的局域网计算机的 IP 地址，然后选中“启用”，最后单击“保存”按钮，即可完成 DMZ 主机的设置。

注意：

设置 DMZ 主机之后，与该 IP 相关的防火墙设置将不起作用。

5.6.4 UPnP设置

选择转发规则下的 UPnP 设置，将进入下面的设置界面。依靠 UPnP（Universal Plug and Play）协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源，例如，Windows XP 和 Windows ME 系统上安装的 MSN Messenger，在使用音频和视频通话时就可以利用 UPnP 协议，这样原本受限于 NAT 的功能便可以恢复正常使用。



- **UPnP 设置列表**　　显示 UPnP 条目信息。
- 应用描述　　显示应用程序通过 UPnP 向路由器请求端口转换时的描述。
- 外部端口　　显示端口转换时采用的路由器端口号。
- 协议类型　　表明是对 TCP 还是 UDP 进行端口转换。
- 内部端口　　显示需要进行端口转换的主机端口号。
- IP 地址　　显示需要进行端口转换的主机 IP 地址。
- 状态　　显示条目状态。“Enabled”表示应用程序请求并启用了端口转换；"Disabled"表示应用程序请求了端口转换，但并没有启用。

举例：

使用 UPnP 的方法如下：

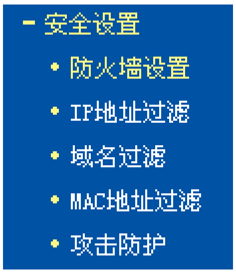
如果您的电脑开启了防火墙功能，请您在 Windows 防火墙界面的例外项中，选则启用 UPnP 框架程序。具体操作方法步骤为：开始→控制面板→安全中心→ Windows 防火墙→例外→选中 UPnP 框架。若例外项中没有 UPnP 项，则点击添加程序，再选中 UPnP 功能即可。

1. 在路由器 UPnP 界面中点击“启用 UPnP”按钮开启 UPnP 功能。
2. 当 MSN Messenger 等程序在运行中使用本功能时，按“刷新”按钮可以看到端口转换信息。端口转换信息由应用程序发出请求时提供。

注意：

- 不使用时请单击“关闭 UPnP”按钮，关闭 UPnP 功能。
- 因为现阶段版本的 UPnP 协议的安全性还未得到充分保证，所以在不需要时请关闭 UPnP 功能。
- 只有支持 UPnP 协议的应用程序才能使用本功能，MSN Messenger 还需要操作系统的支持（如 Windows XP/ME）。

5.7 安全设置



在“安全设置”菜单下面，共有“防火墙设置”、“IP 地址过滤”、“域名过滤”、“MAC 地址过滤”和“攻击防护”五个子项。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.7.1 防火墙设置

选择安全设置下的防火墙设置，将进入下面的设置界面。本节介绍防火墙的各个过滤功能的开启与关闭设置。只有防火墙的总开关是开启的时候，后续的“IP 地址过滤”、“域名过滤”、“MAC 地址过滤”才能够生效，反之，则失效。



- **开启防火墙**　　请选择是否开启防火墙功能。这是防火墙的总开关，当该开关关闭时，“IP 地址过滤”、“域名过滤”、“MAC 地址过滤”功能将全部失效。
- **开启 IP 地址过滤**　　请选择是否开启防火墙的 IP 地址过滤功能，只有选择该项时，IP 地址过滤设置才能生效。
- **开启域名过滤**　　请选择是否开启防火墙的域名过滤功能，只有选择该项时，域名过滤设置才能生效。
- **开启 MAC 地址过滤**　　请选择是否开启防火墙的 MAC 地址过滤功能，只有选择该项时，MAC 地址过滤设置才能生效。
- **开启攻击防护**　　请选择是否开启防火墙的攻击防护功能。

5.7.2　IP地址过滤

选择安全设置下的 IP 地址过滤，将进入下面的设置界面。本页显示已设的 IP 地址过滤列表。可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则；甚至可以通过按钮—“移动”来调整各条过滤规则的顺序，以达到不同的过滤优先级。



- **IP 地址过滤条目表**　　显示 IP 地址过滤条目信息。
- **生效时间**　　显示规则生效的起始时间和终止时间。格式为 hhmm，例如 0803，表示 8 时 3 分。
- 局域网 IP 地址　　显示局域网中被控制的计算机的 IP 地址，为空表示对局域网中所有计算机进行控制。这里可以是一个 IP 地址段，例如 192.168.1.100－192.168.1.200。
- （局域网）端口　　显示局域网中被控制的计算机的服务端口，为空表示对该计算机所有服务端口进行控制。这也可以是一个端口段，例如 1024－8080。
- 广域网 IP 地址　　显示广域网中被控制的网站的 IP 地址，为空表示对整个广域网进行控制。这也可以是一个 IP 地址段，例如 222.88.88.20－222.88.88.222。
- （广域网）端口　　显示广域网中被控制的网站的服务端口，为空表示对该网站的所有服务端口进行控制。这也可以是一个端口段，例如：10-110。

- 协议　　显示被控制的数据包所使用的协议。
- 通过　　显示符合本条目设置规则的数据包是否可以通过路由器。
- 状态　　显示本条目状态，即是否使本条过滤规则生效。
- 配置　　显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**　　点击该按钮，您可以在过滤列表中添加新的过滤条目。详见后面所述。
- **使所有条目生效**　　点击该按钮，您可以设置表中所有过滤条目的状态为“生效”。
- **使所有条目失效**　　点击该按钮，您可以设置表中所有过滤条目的状态为“失效”。
- **删除所有条目**　　点击该按钮，您可以删除当前表中已设的所有过滤条目。
- **移动**　　通过条目序号，您可以将某条记录移动到另一个位置，以达到不同的过滤优先级。

5.7.2.1 添加或编辑IP地址过滤规则

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面。界面中的各参数说明，请见上面 IP 地址过滤条目表所述。



若需要添加新的 IP 地址过滤条目或修改已存的条目，只需要正确设置上面各参数，然后点击保存按钮即可。下面将举例说明。

举例:

设置局域网中 IP 地址为 192.168.1.7 的计算机在 8:00-21:00 时段内不能收发邮件；IP 地址为 192.168.1.8 的计算机全天均不能访问 IP 为 202.96.134.12 的网站，对局域网中的其它计算机则不做任何限制。

设置步骤:

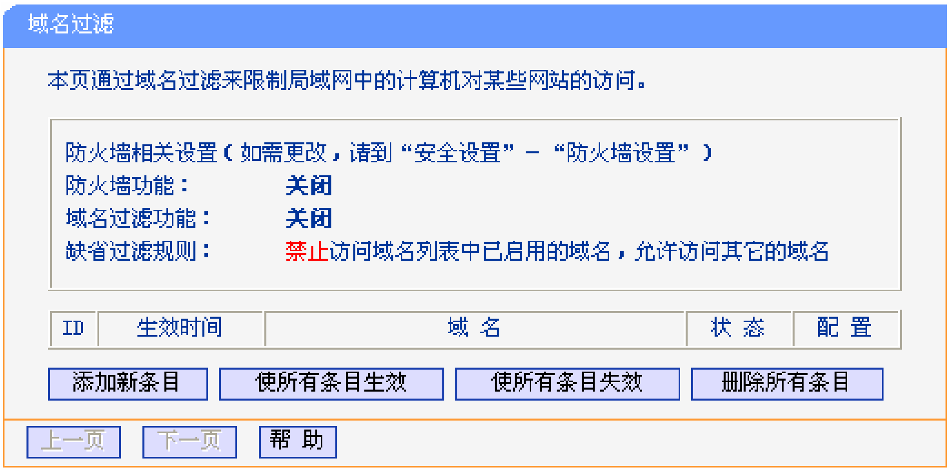
首先请您在“防火墙设置”中打开防火墙总开关，然后再开启“IP 地址过滤”，并设置“缺省过滤规则”为“凡是不符合已设 IP 地址过滤规则的数据包，允许通过本路由器”。最后，在添加或编

辑界面中按照以上数据要求添加新的过滤条目，添加设置界面如上图所示。下面为添加后的 IP 地址过滤条目表。

ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0800-2100	192.168.1.7	-	-	25	ALL	否	生效	编辑 删除
2	0800-2100	192.168.1.7	-	-	110	ALL	否	生效	编辑 删除
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	否	生效	编辑 删除

5.7.3 域名过滤

选择安全设置下的域名过滤，将进入下面的设置界面。本页显示已设的域名过滤列表。可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。



- **域名过滤条目表**　显示域名过滤的条目信息。
- 生效时间　显示规则生效的起始时间和终止时间。格式为 hhmm，例如 0803，表示 8 时 3 分。
- 域名　显示您希望控制的域名。
- 状态　显示本条目状态，即过滤规则是否生效。
- 配置　显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**　点击该按钮，您可以添加新的过滤条目。
- **使所有条目生效**　点击该按钮，您可以将列表中的所有过滤条目的状态设置为“生效”。
- **使所有条目失效**　点击该按钮，您可以将列表中的所有过滤条目的状态设为“失效”。
- **删除所有条目**　点击该按钮，您可以删除该列表中的所有过滤条目。

5.7.3.1 添加或编辑域名过滤规则

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面，界面中各参数说明见前面域名过滤条目表中所述。



举例:

设置局域网中的计算机在 08:00-21:00 时段内不能访问“www.yahoo. com.cn”，08:00-24:00 时段内不能访问“sina.com”，全天不能访问所有以“.net”结尾的网站，这时您需要设置如下的域名过滤表：

设置步骤：

首先在“防火墙设置”中打开防火墙总开关，然后开启“域名过滤”，设置“缺省过滤规则”为“禁止访问域名列表中已启用的域名，允许访问其它的域名”。最后，点击添加新按钮，在添加或编辑界面中按照以上数据要求设置新的域名过滤条目，设置界面如上图所示。下面为添加后的 IP 地址过滤条目表。

ID	生效时间	域 名	状 态	配 置
1	0800-2100	www.yahoo.com.cn	生效	编辑 删除
2	0800-2400	sina.com	生效	编辑 删除
3	0000-2400	.net	生效	编辑 删除

5.7.4 MAC地址过滤

选择安全设置下的域名过滤，您将进入下面的设置界面。本页显示已设的 MAC 地址过滤列表。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。

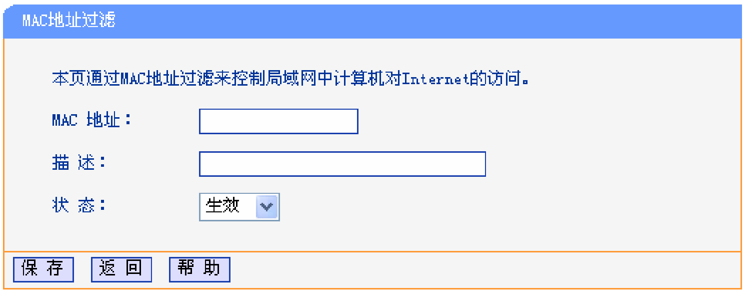


- **MAC 地址过滤表**　显示 MAC 地址过滤条目信息。
- MAC 地址　显示您希望控制的计算机的 MAC 地址。
- 描述　显示对该计算机的适当描述。
- 状态　显示本条目状态，即本条过滤规则是否生效。

- 配置　　　　　显示对该条目操作的超级链接——编辑或删除。
- **添加新条目**　　　点击该按钮，您可以在过滤列表中添加新的过滤条目。
- **使所有条目生效**　　点击该按钮，您可以将该列表中所有过滤条目的状态设为“生效”。
- **使所有条目失效**　　点击该按钮，您可以将该列表中所有过滤条目的状态设为“失效”。
- **删除所有条目**　　点击该按钮，您可以删除当前已设的所有过滤条目。

5.7.4.1 添加或编辑MAC地址过滤规则

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，您将进入下面的设置界面，界面中各参数说明见前面 MAC 地址过滤条目表中所述。



举例:

设置局域网中 MAC 地址为 00-13-8F-A9-E6-CB 和 00-13-96-6B-6E-A9 的计算机不能访问 Internet，局域网中的其它计算机能访问 Internet，这时您需要设置如下的 MAC 地址过滤表。

设置步骤:

首先在“防火墙设置”中打开防火墙总开关，然后开启“MAC 地址过滤”，设置“缺省过滤规则”为“禁止已设 MAC 地址列表中已启用的 MAC 地址访问 Internet，允许其它 MAC 地址访问 Internet”。然后，点击添加新条目按钮，类似上面界面所示设置各条目参数，设置完后点击保存。最后形成的 MAC 地址过滤条目表为:

ID	MAC地址	描 述	状 态	配 置
1	00-13-8F-A9-E6-CB	张三的计算机	生效	编辑 删除
2	00-13-96-6B-6E-A9	李四的计算机	生效	编辑 删除

5.7.5 攻击防护

选择安全设置下的攻击防护，将进入下面的攻击防护的设置界面。攻击防护是防火墙通过对数据包的检查，以应对一些恶意的攻击。攻击检查和防护分为四类:

- 扫描类攻击防护
- 拒绝服务（DoS）攻击防护
- 可疑包攻击防护
- 含有 IP 选项的包的攻击防护

如果在数据包中查到符合指定的攻击模式，则进行相应的防护处理。设置界面如下图所示。



5.7.5.1 区域设置

区域设置表明，后续的攻击防护设置项，是对应来自指定区域的数据包进行监控。如选中 LAN，则表示对来自局域网的数据包进行监控，如上图。

5.7.5.2 扫描类攻击防护

扫描类攻击防护包括三种类型：IP 扫描、端口扫描、IP 欺骗。

IP 扫描

该项用来检查在小于规定的时间内，是否存在从一个源 IP 地址发送 ICMP 请求包到 10 个不同的目的 IP 地址的现象。如果有，则认为此源 IP 正在进行 IP 扫描攻击。选中 IP 扫描复选框，表明对来自指定区域（见区域设置节）的包进行 IP 扫描攻击的检查，设置阈值指明规定的时间间隔。阈值选择范围为 2000-1000000 微秒。如果欲取消对来自指定区域的包进行 IP 扫描攻击的检查，则清除 IP 扫描选择即可。

端口扫描

该项用来检查在小于规定的时间内，是否存在从一个源 IP 地址发送 TCP SYN 包到同一目的地址的 10 个不同端口的现象。如果有，则认为此源 IP 正在进行端口扫描攻击。选中端口扫描复选框，表明对来自指定区域的包进行端口扫描攻击检查，设置阈值指明规定的时间间隔，阈值选择范围为 2000-1000000 微秒。如果欲取消对来自指定区域的包进行端口扫描攻击检查，则清除端口扫描选择即可。

IP 欺骗（仅针对局域网）

发出攻击的主机通常使用假 IP 地址作为自己的源地址，从而使得被攻击方不能查到真正的攻击者。选中 IP 欺骗复选框，表明对来自指定区域的包进行 IP 欺骗检查。如果欲取消对来自指定区域的包进行 IP 欺骗检查，则清除 IP 欺骗选择即可。

⚠ **注意:**

本功能仅在区域为 LAN 时有效，在区域为 WAN 时是无效的。

5.7.5.3 DoS类攻击防护

DoS 类攻击防护包括五种类型：ICMP Flood、UDP Flood、SYN Flood、Land Attack、WinNuke。

ICMP Flood 攻击

该项用来检查在一秒钟内，一个目的 IP 是否收到超过规定数量的 ICMP 请求包。如果收到超过规定数量的包，则认为此目的 IP 正受到 ICMP Flood 的攻击。选中 ICMP Flood 复选框，表明对来自指定区域的包进行 ICMP Flood 攻击检查。设置阈值指明一秒内收到的包数（Packets Per Second），其范围为 10-99999 PPS。如果欲取消对来自指定区域的包进行 ICMP Flood 攻击检查，则清除 ICMP Flood 选择即可。

UDP Flood 攻击

该项用来检查在一秒钟内，一个目的 IP 的某一端口是否收到超过规定数量的 UDP 包。如果收到超过规定数量的包，则认为此目的 IP 的此端口正受到 UDP Flood 的攻击。选中 UDP Flood 复选框，表明对来自指定区域的包进行 UDP Flood 攻击检查。设置阈值指明一秒内收到的包数，范围为 10-99999 PPS。如果欲取消对来自指定区域的包进行 UDP Flood 攻击检查，则清除 UDP Flood 选择即可。

SYN Flood 攻击

该项用来检查在一秒钟内，一个目的 IP 的某一端口是否收到超过规定数量的 TCP SYN 包。如果收到超过规定数量的包，则认为此目的 IP 的此端口正受到 SYN Flood 的攻击。选中 SYN Flood 复选框，表明对来自指定区域的包进行 SYN Flood 攻击检查。设置阈值指明一秒内收到的包数，范围为 10-99999 PPS。如果欲取消对来自指定区域的包进行 SYN Flood 攻击检查，则清除 SYN Flood 选择即可。

LAND 攻击

该项用来检查将 SYN Flood 攻击和 IP 欺骗结合在一起的攻击，当攻击者发送含有受害者 IP 地址的欺骗性 SYN 封包，将其作为目的和源 IP 地址时，就发生了 LAND 攻击。选中 LAND Attack 复选框，表明对来自指定区域的包进行 Land 攻击检查。如果欲取消对来自指定区域的包进行 LAND 攻击检查，则清除 LAND Attack 选择即可。

WinNuke

WinNuke 是针对网上运行 Windows 的任何计算机的 DoS 攻击。攻击者将 TCP 片段（通常给设置了紧急[URG]标志的 NetBIOS 端口 139）发送给已建连接的主机。这样就产生 NetBIOS 碎片重叠，从而导致运行 Windows 的机器崩溃。选中 WinNuke 复选框，表明对来自指定区域的包进行 WinNuke 攻击检查。如果欲取消对来自指定区域的包进行 WinNuke 攻击检查，则清除 WinNuke 选择即可。

5.7.5.4 可疑包类防护

可疑包类防护包括五类：大的 ICMP 包（大于 1024 字节）、没有 Flag 的 TCP 包、同时设置 SYN 和 FIN 的 TCP 包、仅设置 FIN 而没有设置 ACK 的 TCP 包、未知协议。

大的 ICMP 包（ 大于 1024 字节）

正常的 ICMP 数据包长度较小，一般不会大于 1024 字节。选中大的 ICMP 包（大于 1024 字节）复选框，表明对来自指定区域的包进行 ICMP 包合法性检查。如果欲取消对来自指定区域的包进行大的 ICMP 包（大于 1024 字节）检查，则清除相应选项的选择即可。

没有 Flag 的 TCP 包

正常的 TCP 包的包头至少设置有一个标志（flag）。未设置任何控制标志的 TCP 包是一个可疑包。选中没有 Flag 的 TCP 包复选框，表明对来自指定区域的包进行没有 Flag 的 TCP 包检查。如果欲取消对来自指定区域的包进行没有 Flag 的 TCP 包检查，则清除相应选项的选择即可。

同时设置 SYN 和 FIN 的 TCP 包

TCP 包头的 SYN 标志同步发起 TCP 连接的序列号，FIN 标志表示完成 TCP 连接的数据传输的结束。两个标志的用途是互相排斥的。在同一 TCP 片段包头中同时设置 SYN 和 FIN 控制标志是异常的 TCP 包。选中同时设置 SYN 和 FIN 的 TCP 包复选框，表明对来自指定区域的包进行同时设置 SYN 和 FIN 的 TCP 包检查。如果欲取消对来自指定区域的包进行同时设置 SYN 和 FIN 的 TCP 包检查，则清除相应选项的选择即可。

仅设置 FIN 而没有设置 ACK 的 TCP 包

含有 ACK 标志的 TCP 包是确认接收到的前一个包。含有 FIN 标志的 TCP 包是发送会话结束信号并终止连接，它通常也设置了 ACK 标志。设置了 FIN 标志，而未设置 ACK 标志的 TCP 包是异常的 TCP 包。选中仅设置 FIN 而没有设置 ACK 的 TCP 包复选框，表明对来自指定区域的包进行仅设置 FIN 而没有设置 ACK 的 TCP 包检查。如果欲取消对来自指定区域的包进行仅设置 FIN 而没有设置 ACK 的 TCP 包检查，则清除相应选项的选择即可。

未知协议

目前，IP 包头的协议类型（protocol type）字段保留大于 135（包括 135）的数值未定义。正是由于这些协议未定义，就无法事先知道某一特定的未知协议是善意的还是恶意的。对这些非标准协议，谨慎的态度是封锁这类未知的元素进入受保护网络。选中未知协议复选框，表明对来自指定区域的包进行未知协议检查。如果欲取消对来自指定区域的包进行未知协议检查，则清除相应选项的选择即可。

5.7.5.5 含有IP选项的包防护

在 Internet Protocol 协议（RFC 791）中，指定了一组选项以提供特殊路由控制、诊断工具和安全性。它是在 IP 包头中的目的地址之后。协议认为这些选项“对最常用的通信是不必要的”。在实际使用中，它们也很少出现在 IP 包头中。这些选项经常被用于某些恶意用途。

IP 选项包括：

- **IP Timestamp Option**　　表明是否检查来自指定区域的 IP 包含有 Internet Timestamp 项
- **IP Security Option**　　表明是否检查来自指定区域的 IP 包含有 Security 项
- **IP Stream Option**　　表明是否检查来自指定区域的 IP 包含有 Stream ID 项
- **IP Record Route Option**　　表明是否检查来自指定区域的 IP 包含有 Record Route 项
- **IP Loose Source Route Option**　　表明是否检查来自指定区域的 IP 包含有 Loose Source Route 项
- **IP Strict Source Route Option**　　表明是否检查来自指定区域的 IP 包含有 Strict Source Route 项
- **非法 IP 选项**　　表明是否检查来自指定区域的 IP 包的完整性或正确性

选中一项 IP 选项的复选框，则检查；清除选项的选择，则取消检查。

5.8 路由功能



在“路由功能”菜单下面，只有“静态路由表”一个子项。单击该子项，即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

5.8.1 静态路由表

选择路由功能下的静态路由表项，将进入下面所示界面。本页设置路由器的静态路由功能，可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。



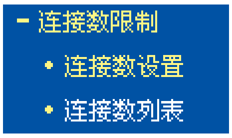
- **静态路由表**　　显示静态路由条目表中的信息。
- 目的 IP 地址　　显示欲访问的主机的 IP 地址。
- 子网掩码　　显示子网掩码，一般为 255.255.255.0。
- 网关　　显示数据包被发往的路由器或主机的 IP 地址。
- 状态　　显示本条目的状态，即本条目是否生效。

- 配置　　　　　显示对本条目操作的超级链接——编辑或删除。
- 添加新条目　　点击该按钮，可以在路由列表中添加新的条目。
- 使所有条目生效　点击该按钮，可以将列表中所有条目的状态设为“生效”。
- 使所有条目失效　点击该按钮，可以将列表中所有条目的状态设为“失效”。
- 删除所有条目　点击该按钮，可以删除当前列表中已设的所有条目。

当点击“添加新条目”或点击“编辑”链接界面时，将进入下面的设置界面。



5.9 连接数限制



在“连接数限制”菜单下面，共有“连接数设置”、“连接数列表”两个子项。

单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.9.1 连接数设置

选择连接数限制下的连接数设置，将进入连接数设置界面。本页设置单机的连接数限制，对指定 IP 地址的计算机连接数进行限制，超过限制的新连接不允许通过路由器，未设置限制的计算机可以不受限制的建立连接。您可以利用按钮—“添加新条目”来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。如下图示：



- 连接数限制　　您可以选择是否开启连接数限制功能。
- 连接数限制列表　显示已经设置的连接数限制条目。

- 局域网 IP 地址　　显示您希望限制的计算机的 IP 地址。可以输入一个 IP 地址段，例如：192.168.1.20-192.168.1.30，也可以只输入一个 IP 地址，例如：192.168.1.40。
- 最大连接数　　显示允许该计算机建立的最大连接数。
- 启用　　显示该条目的限制是否生效。
- **添加新条目**　　点击该按钮，您可以在列表中添加新的条目。
- **删除所有条目**　　点击该按钮，您可以删除列表中的所有条目。

点击“添加新条目”或点击“编辑”链接时的界面，将进入下面的设置界面。可以添加一条新的连接数限制条目，也可以编辑已经存在的限制条目。



5.9.2　连接数列表

选择连接数限制下的连接数列表，您将进入下面所示界面。本页显示已设置的连接数和当前通过路由器的所有连接数，下图只显示了连接数列表中的部分数据。



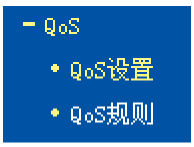
连接数列表

本页显示连接数列表。
局域网地址总数：22　当前总连接数：1

ID	局域网IP地址	最大连接数	当前连接数
1	192.168.1.23	200	1
2	192.168.1.11	200	0
3	192.168.1.10	200	0
4	192.168.1.13	200	0
5	192.168.1.12	200	0
6	192.168.1.15	200	0

- 局域网 IP 地址　　客户端的 IP 地址。
- 最大连接数　　设定的连接数限制，如果没有设置限制则显示“无限制”。
- 当前连接数　　该客户端当前有效的连接数。

5.10　QoS



在“QoS”菜单下面，共有“QoS 设置”、“QoS 规则”两个子项。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.10.1 QoS设置

选择 QoS 下的 QoS 设置，将进入下面所示界面。本页主要对 QoS 的开启与关闭进行设置。



- 开启功能 请您选择是否开启 QoS 设置，选中该复选框则表示启用该功能。
- 上行总带宽 请您输入希望路由器通过 WAN 口提供的上传速率，最大值为 100000Kbps。
- 下行总带宽 请您输入希望路由器通过 WAN 口提供的下载速率，最大值为 100000Kbps。

注意:

只有 QoS 的总开关开启时，后续的“QoS 规则”才能够生效，反之，则无效。

5.10.2 QoS规则

选择 QoS 下的 QoS 规则，将进入下面所示界面。QoS 规则分为 QoS 规则列表和 QoS 规则配置。



在 QoS 规则列表中，可以查看用户创建的全部规则。每个规则包含的条目有：

- **QoS 规则列表** 显示用户创建的所有规则信息。每个规则包含的条目有
- ID 规则序号。
- 描述 显示描述的信息，包括地址段，传输层的端口段和协议；其格式有：地址段/端口段/协议，端口段/协议，端口段，地址段。
- 模式 显示带宽的使用形式，分为独立带宽和共享带宽；独立带宽表示地址或端口各自拥有上下行带宽值，共享带宽表示地址或端口共享上下行带宽值。
- 上行带宽 显示 WAN 口允许的最大上传速度限制和最小上传速度保证，为 0 时表示采用缺省值。输入范围为 0-100000Kbps。
- 下行带宽 显示 WAN 口允许的最大下载速度限制和最小下载速度保证，为 0 时表示采用缺省值。输入范围为 0-100000 Kbps。

- 启用　　显示规则的状态，选中该复选框则表示该规则生效。
- 配置　　显示可以对该规则进行的超级链接——编辑或删除。
- **添加新条目**　　点击该按钮，可以添加新的 QoS 规则。
- **删除所有条目**　　点击该按钮，可以删除列表中的所有规则条目。

点击 QoS 规则列表中的添加新条目或编辑按钮，将进入下面的设置界面。在 QoS 规则配置中，可以创建新的 QoS 规则或修改已存在的规则。具体设置见下图示。



- 启用　　请您选择是否启用该规则。
- IP 地址段　　请您输入内部主机的地址范围。当全部为空或为 0.0.0.0 时表示该域无效。
- 端口段　　请您输入内部主机访问外部服务器的端口范围。当全部为空或为 0 时表示该域无效。
- 协议　　请您输入传输层采用的协议类型，这里有 ALL(任意匹配)、TCP 和 UDP；该域只有在端口段选中下才有效。
- 模式　　请您选择该条规则下，带宽使用的模式，即独立或共享带宽。
- 上行带宽、下行带宽　　请您参考 QoS 规则列表中所述来设置。

5.11 IP与MAC绑定



在“IP 与 MAC 绑定”的菜单下面，有“静态 ARP 绑定设置”、“IP 与 MAC 扫描”和“ARP 映射表”三个子项。单击某个子项，即可进行相应功能的设置，下面将详细讲解各个子项的功能。

5.11.1 静态ARP绑定设置

选择 IP 与 MAC 绑定下的静态 ARP 绑定设置，即可进入该项的设置界面。ARP 绑定是指，指定的 IP 地址的主机在向路由器发送 arp 请求时，当 MAC 地址与绑定的 MAC 地址相同时，才允许其通过路由器，否则不允许使用该 IP 地址的主机发送的 arp 请求通过路由器。ARP 绑定功能分为两种：普通绑定和强制绑定。其中普通绑定允许您限制计算机使用 IP 地址，强制绑定允许您限制计算机的上网行为。

本页显示已经设置的 ARP 静态列表。可以利用按钮“增加单个条目”来增加新的 ARP 静态条目，或者通过按钮“编辑”或“删除”链接来修改或删除旧的 ARP 静态条目。

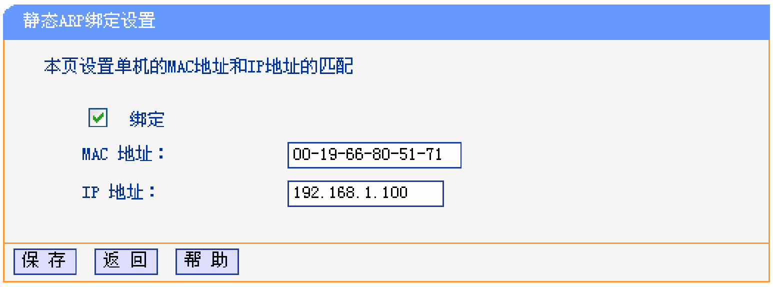
要使用 ARP 绑定功能，需要先设置以下项目：



- **ARP 绑定**　ARP 绑定功能分为两种：普通绑定和强制绑定。默认状态下 ARP 绑定功能未启用，如需应用，请选择一种 ARP 绑定功能，按下“保存”按钮后，ARP 绑定功能生效。
- 普通绑定　用于限制计算机使用 IP 地址。只允许指定 MAC 地址的计算机使用指定的 IP 上网，其他计算机不用能使用该 IP 上网。
- 强制绑定　用于限制计算机的上网行为。只允许条目中绑定了 MAC 地址和 IP 地址的计算机上网，其他计算机不能上网。
- **静态 ARP 绑定列表**　显示 IP 与 MAC 地址绑定的条目信息。
- MAC 地址　显示您希望控制的计算机的 MAC 地址。
- IP 地址　显示您希望与指定 MAC 地址绑定的 IP 地址。
- 绑定　显示该条目的状态，选中该复选框则表示绑定条目生效。
- 编辑　显示对该绑定条目操作的超级链接——编辑或删除。
- **增加单个条目**　点击该按钮，您可以在静态绑定列表中添加新的条目。
- **删除所有条目**　点击该按钮，您可以删除静态列表中的所有条目。
- **查找指定条目**　点击该按钮，您可以在静态列表中查找指定 IP 地址或 MAC 地址的条目。具体查找方法见后面所述。
- **使所有条目生效**　点击该按钮，您可以使当前静态列表中的所有绑定条目生效。

5.11.1.1 添加或编辑静态ARP绑定条目

添加或编辑静态 ARP 绑定条目时，请点击上图所示界面中的“增加单个条目”或“编辑”按钮，可以进入下面的设置界面。



举例:

设置只允许局域网中 MAC 地址为 00-19-66-80-51-71 的计算机使用 IP 地址 192.168.1.100，其他计算机不能使用该 IP 地址。

设置步骤如下:

首先，请设置该节首页中的“ARP 绑定”为“普通绑定”，并保存。

然后请点击“增加单个条目”按钮，并按上图设置添加新的静态绑定条目。最后按下保存即可。

您也可以通过条目上配置中的“编辑”按钮，对已经设置的条目进行编辑，其界面与上图相同。

举例:

设置只允许局域网中 MAC 地址为 00-19-66-80-51-71 且 IP 地址 192.168.1.100，其他计算机不能上网。

设置步骤如下:

首先，请点击“增加单个条目”按钮，并按上图设置添加新的静态绑定条目。最后按下保存即可。

然后，请设置该节首页中的“ARP 绑定”为“强制绑定”，并保存。

注意:

开启强制绑定功能时，必须确保当前登录路由器的管理计算机已经设置了 MAC 和 IP 绑定条目，并且该条目已经绑定。否则启用该功能后，您的计算机将不能继续登录路由器，也不能上网。

5.11.1.2 查找静态ARP绑定条目

如果您希望查找特定的 IP 地址或 MAC 地址是否已经设置到静态绑定表中，您可以在首页中点击“下一页”、“上一页”按钮或直接选择指定页进行浏览查找。另外，您也可以点击按钮“查找指定条目”进入到下图界面中进行快速查找。



举例:

例如您要查找 IP 地址为 192.168.1.100 的条目。

查找步骤如下:

首先，请单击按钮“查找指定条目”，然后进入下图设置查找信息，您可以在 IP 地址栏中输入 192.168.1.100 进行查找。



最后，单击按钮“查找”，则可以得到结果。

在上图中，如果您需要对该条目进行进一步的编辑操作，可以点击上图所示界面中的链接——“转至该页”按钮，进入该条目所在的 ARP 静态绑定列表所在页（条目呈黄色高亮），再选择条目旁边的“编辑”按钮，进入编辑界面对它进行编辑。如下图示:



5.11.2 IP与MAC扫描

您可以使用 IP 与 MAC 扫描功能方便地设置 ARP 绑定条目。该可以自动扫描指定 IP 范围内的计算机的 MAC 地址，并可以通过选择，一键式地绑定扫描获得的条目。



➢ MAC 地址　　网络中某台计算机的 MAC 地址。

➢ IP 地址　　该计算机当前使用的 IP 地址。

➢ 状态　　该计算机的 MAC 与 IP 是否被绑定。

➢ 选择　　在选项框中打勾，即可使用添加选定条目按钮导入该条目。

➢ **全部选定**　　自动选中当前显示的所有条目。

➢ **全部不选**　　取消对当前显示的所有条目的选择。

➢ **添加选定条目**　　向 ARP 绑定表中导入选中的所有条目。

5.11.3 ARP映射表

选择 IP 与 MAC 绑定下的 ARP 映射表，可以进入 ARP 映射表显示界面。本页显示当前设置的和通过路由器 ARP 的映射列表，并显示是否已经绑定。同时也可以将指定映射条目导入到 ARP 静态列表中进行进一步的编辑操作，或者直接删除该映射条目。



➢ **ARP 映射表**　　显示映射表条目信息。

➢ MAC 地址　　显示网络中计算机的 MAC 地址。

➢ IP 地址　　显示与 MAC 地址匹配的计算机的 IP 地址。

➢ 状态　　显示该条目状态，绑定或未绑定。

➢ **配置**　　显示对该条目的操作的超级链接——导入或删除。

➢ 导入　　点击该按钮，可以将该条目导入到前面的静态 ARP 绑定列表中。

➢ 删除　　点击改按钮，可以将该条目从 ARP 映射表中删除。

注意：

只有静态 ARP 绑定设置界面选择了普通绑定或强制绑定，且条目已经绑定时，ARP 映射表中对应条目的状态才会显示“已绑定”。

ARP 映射表中的条目状态为“已绑定”时，点击其右侧的“删除”，ARP 映射表及静态 ARP 绑定列表中对应的条目状态都将由“绑定”变成“不绑定”。

ARP 映射表中的条目状态为“不绑定”时，其右侧的“删除”不起任何作用。

- 全部绑定　　点击该按钮，可以动态绑定当前列表中所有条目(不保存到静态 ARP 绑定列表中)。
- 全部导入　　点击改按钮，可以把当前 ARP 映射表的所有条目全部导入到静态 ARP 绑定列表中，如果有冲突条目，将忽略冲突条目，添加其他条目；如果静态绑定表已满，则忽略多余的条目。

5.12 花生壳DDNS

DDNS 又名动态 DNS，它的主要功能是实现固定域名到动态 IP 地址之间的解析。对于使用动态 IP 地址的用户，在每次上网得到新的 IP 地址后，安装在主机上的动态域名软件就会将该 IP 地址发送到由 DDNS 服务商提供的动态域名解析服务器，并更新域名解析数据库。当 Internet 上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的 IP 地址。这样，大多数不使用固定 IP 地址的用户，也可以通过动态域名解析服务经济、高效地构建自身的网络系统。

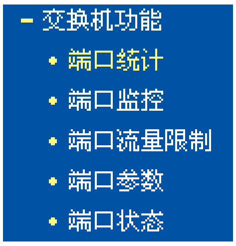
选择花生壳 DDNS 菜单，在界面的“服务提供者”下拉选项中选择“花生壳（www.oray.net）”，将进入下图所示的花生壳 DDNS 设置界面。本页设置“花生壳”的 DDNS 参数，当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式对您的路由器或虚拟服务器进行访问了。



- 服务商链接　　成功连接外网后，点击该项，可以分别链接到“花生壳动态域名解析服务申请”和“花生壳动态域名解析服务帮助”页面。
- 服务提供者　　请您选择提供 DDNS 的服务器名。
- 用户名　　请您输入在 DDNS 服务器上注册的用户名。

- 密码　　　　请你输入在 DDNS 服务器上注册的密码。
- 启用 DDNS　　请您选择是否启用该 DDNS 功能。
- 连接状态　　显示当前与 DDNS 服务器的连接状态。
- 服务类型　　显示当前用户的类型。
- 域名信息　　显示当前 DDNS 服务器获得的域名服务列表。

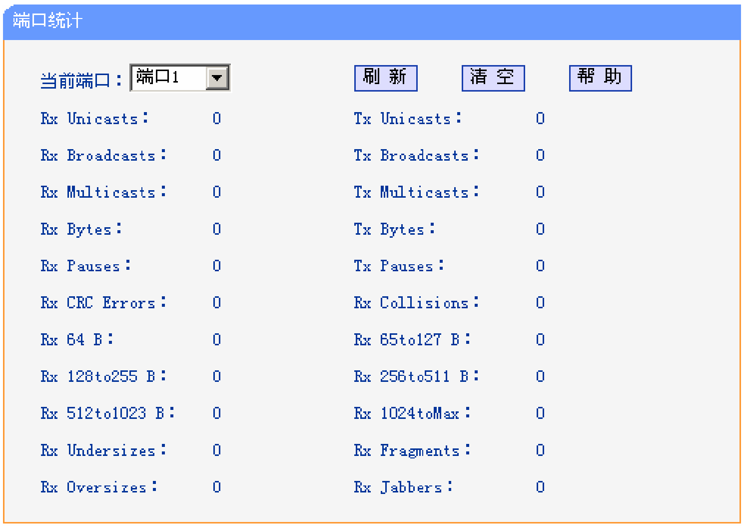
5.13 交换机功能



在“交换机功能”菜单下面，共有“端口统计”、“端口监控”、“端口流量限制”、“端口参数”、“端口状态”五个子项。单击某个子项，即可进行相应的功能设置或查询相关的状态，下面将详细讲解各子项的功能。

5.13.1 端口统计

选择交换机功能下的端口统计，可以进入端口统计显示界面。端口统计将针对每一个端口，统计它收发了多少数据字节、多少数据帧、多少个广播帧、多少个多播帧、多少个错误帧等等。其页面显示如下：



- **Rx Unicasts**　　接收的数据帧的目的 MAC 地址为单播 MAC 地址的数据帧数目。
- **Tx Unicasts**　　发送的数据帧的目的 MAC 地址为单播 MAC 地址的数据帧数目。
- **Rx Broadcasts**　　接收的数据帧的目的 MAC 地址为广播 MAC 地址的数据帧数目。
- **Tx Broadcasts**　　发送的数据帧的目的 MAC 地址为广播 MAC 地址的数据帧数目。

- **Rx Multicasts** 接收的数据帧的目的 MAC 地址为多播 MAC 地址的数据帧数目。
- **Rx Bytes** 接收的数据帧的总字节数（不包含错误帧）。
- **Tx Bytes** 发送的数据帧的总字节数（不包含错误帧）。
- **Rx Pauses** 接收的 Pause 帧的数据帧数目。
- **Tx Pauses** 发送的 Pause 帧的数据帧数目。
- **Rx CRC Errors** 接收的含非法校验字段的数据帧数目。
- **Rx Collisions** 接收数据帧时产生的碰撞（即冲突）数目。
- **Rx 64 B** 接收及转发的长度为 64 字节的数据帧数目（包含错误帧）。
- **Rx 65to127 B** 接收及转发的长度为 65～127 字节的数据帧数目（包含错误帧）。
- **Rx 128to255 B** 接收及转发的长度为 128～255 字节的数据帧数目（包含错误帧）。
- **Rx 256to511 B** 接收及转发的长度为 256～511 字节的数据帧数目（包含错误帧）。
- **Rx 512to1023 B** 接收及转发的长度为 512～1023 字节的数据帧数目（包含错误帧）。
- **Rx 1024toMax** 接收及转发的长度为 1024～1518 字节的数据帧数目（包含错误帧）。
- **Rx Undersizes** 接收的长度小于 64 字节并且包含合法校验字段的数据帧数目。
- **Rx Fragments** 接收的长度小于 64 字节并且包含非法校验字段的数据帧数目。
- **Rx Oversizes** 接收的长度超过最大字节数并且包含合法校验字段的数据帧数目。
- **Rx Jabbers** 接收的长度超过最大字节数并且包含非法校验字段的数据帧数目。

注意:

以太网中的数据帧长度一般在 64 到 1522 字节之间，本设备支持最大帧长为 1522（IEEE Tag 帧）或 1518（untag 帧）的数据帧的统计，超出这个长度的数据帧将被统计成错误帧（Jumbo 帧除外）。

5.13.2 端口监控

端口监控主要是使用一个监控端口对一个或多个被监控端口进行输出监控（Egress）或输入输出监控（Ingress & Egress）。

页面显示如下图：

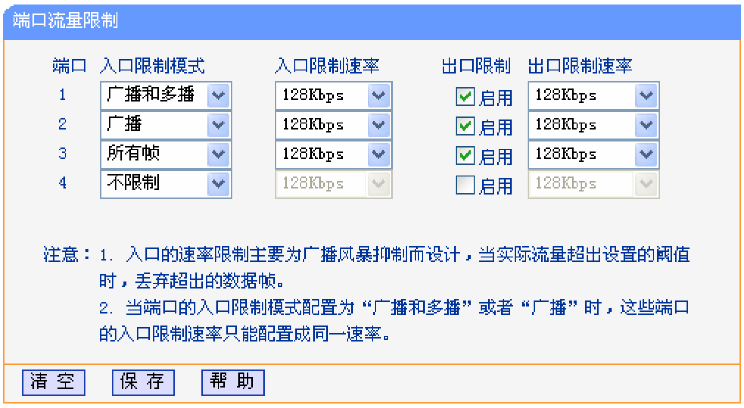


- **监控设置**　　本选项分别是禁用、输入监控、输出监控和输入输出监控。这里的输入/输出是相对路由器的交换机部分而言的。
- **监控端口**　　接有监控主机的端口。
- **被监控端口**　　采用复选的方式可以选择一到四个端口为被监控端口。

5.13.3　端口流量限制

选择交换机功能下的端口流量限制，您可以进入如下设置界面。端口流量限制提供针对每个端口的流量限制设置，入口提供“不限制”、“广播和多播”、“广播”、“所有帧”等五种不同的限制模式，而出口限制则是针对所有帧的限制。

页面显示如下图：



- **入口限制模式**　　请您选择入口限制模式，它一共包含下面五个选项。
- 不限制　　选择该项表示对进入该端口的数据帧不进行限制。
- 广播和多播　　选择该项表示对进入该端口的广播帧和多播帧进行限制。
- 广播　　选择该项表示对进入该端口的广播帧进行限制。
- 所有帧　　选择该项表示对进入该端口的所有帧进行限制。

其中广播以及广播和多播的限制方式就是传统意义上的广播风暴抑制，路由器的交换机部分可以对三种常见的广播帧（广播包、组播包、未学习到地址的单播包）进行过滤。

广播风暴是指网络上的广播帧数量急剧增加而影响正常的网络通讯的反常现象。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧，广播风暴会严重降低网络性能。端口流量限制允许交换机部分对网络上出现的广播帧进行过滤。当设备检测到广播帧数目超出一定的范围时，会自动丢弃广播帧，以防止广播风暴的发生。

当设置为所有帧的限制方式时，交换机部分将对所有的数据帧都进行限制，对于入口的数据包采用过滤处理，若当前流量超出入口限制流量时，超出的部分将被丢弃；对于出口的数据，仅限制流量（根据端口流量控制的开启情况决定是否丢弃超出限制速率外的帧），这时起到端口下行带宽限制的作用。

5.13.4 端口参数

选择交换机功能下的端口参数，可以进入如下设置界面。它主要包括是否启用端口，是否启用端口流量控制，以及设置端口工作模式。

5.13.4.1 端口的工作模式

TL-R4148的交换机部分支持五种端口工作模式：10M 半双工，10M 全双工，100M 半双工，100M 全双工和自协商模式。

如 100M 全双工，前面的数字表示的是传输速率，后面表示的是双工模式。半双工是指传输的两边既可以发送，也可以接收，但是在某一时刻只能有一个设备使用网络传输介质，即不能同时进行发送和接收；全双工是指传输的两边可以同时进行发送和接收，互不影响。

页面显示如下图：



5.13.4.2 端口的N-Way自动协商功能

N-Way自协商功能使端口可根据另一端设备的连接速度和双工模式，自动调节速度和双工模式到双方都可以达到的最高水平。自协商的设备可以交换关于各自功能的信息，这样就可以使设备进行自动配置，实现自动调整传输方式（全双工或半双工）和传输速度（10Mbps，100Mbps）的功能。

5.13.4.3 流量控制

流量控制（Flow control）是为了同步接收方和发送方的的速度而进行的控制。当接收方接收能力比发送方的发送能力小的时候，如果没有流量控制就会丢失数据。流量控制主要分两种情况：在半双工方式下，流控采用 Backpressure 标准；在全双工方式下，使用基于 PAUSE 帧的流量控制，即 IEEE802.3x 标准。

半双工方式下，当接收方设备的资源不足时就会启动流量控制，发送一组载波信号脉冲串（假冲突信号），发送方设备检测到网络上的载波信号和自己发送的信号不同，就会停止一段时间（随机时间）后再发送数据，接收方就可以在这个时间内处理数据，从而达到流量控制。

全双工方式下，当接收方设备的资源不足时就会启动流量控制。由于发送方发送数据时接收方也可以发送数据给发送方（全双工的特征），因此接收方可以通过发送一个 PAUSE 帧告诉发送方停止一段时间再发送数据。这就是全双工下流量控制下的 IEEE802.3x 标准。

5.13.5 端口状态

选择交换机功能下的端口参数，您可以进入如下端口状态显示界面。端口状态可以标识端口上是否接有设备，如果接有设备，它的工作速率是多少，它是工作在全双工模式还是半双工模式，它是否启用了流量控制等等。

页面显示如下图：

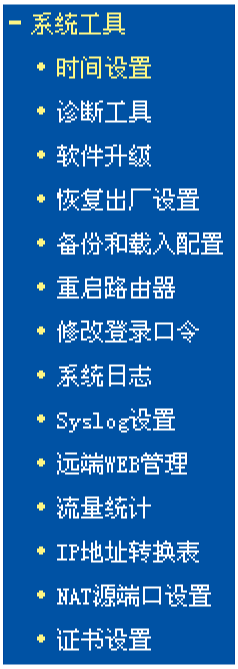


端口状态

端口	端口状态	连接速率(Mbps)	双工模式	流量控制
1	已连接	100	全双工	启用
2	未连接	--	--	--
3	未连接	--	--	--
4	未连接	--	--	--

刷新

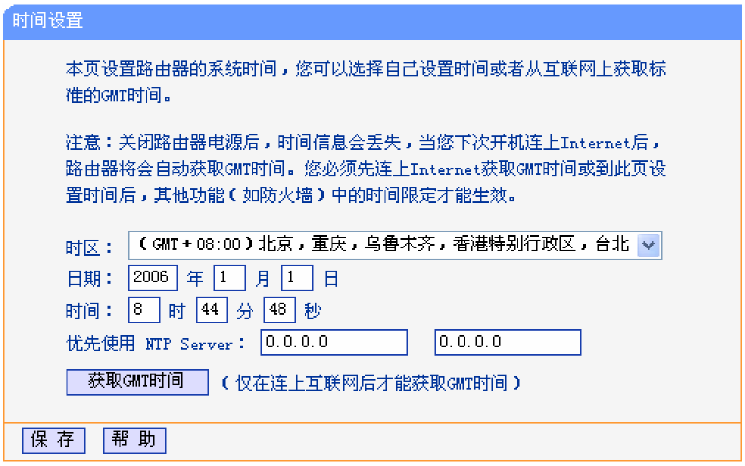
5.14 系统工具



在“系统工具”菜单下面，共有“时间设置”、“诊断工具”、“软件升级”、“恢复出厂设置”、“备份和载入配置”、“重启路由器”、“修改登录口令”、“系统日志”、“Syslog 设置”、“远端 WEB 管理”、“流量统计”、“IP 地址转换表”、“NAT 源端口设置”、“证书设置”14 个子项。单击其中某个子项，即可对它进行相应的功能设置，下面将详细讲解各子项的功能。

5.14.1 时间设置

选择系统工具下的时间设置，可以进入下面的时间设置界面。本页用来设置路由器的系统时间，您可以选择自己设置时间，也可以选择从互联网上获取标准的 GMT 时间。具体设置页面如下：



➢ 优先使用 NTP Server　请输入希望采用的 NTP Server 的 IP 地址（可以输入两个）。NTP Server 是网络时间服务器，用于 Internet 网上的计算机时间同步。当路由器获取 GMT 时间时，优先从该时间服务器上获取。

举例:

系统时间设置步骤:

首先请您选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击保存按钮完成系统时间的设置。

如果您已经连上了互联网，则您也可以直接单击获取 GMT 时间按钮，从互联网上获取标准的 GMT 时间。

注意:

关闭路由器电源后，时间信息会丢失，只有当您下次开机连上 Internet 后，路由器才会自动获取 GMT 时间。

您必须先连上 Internet 获取 GMT 时间或在此页手动设置系统时间，路由器其他功能（如防火墙）中的时间限定才能生效。

5.14.2　诊断工具

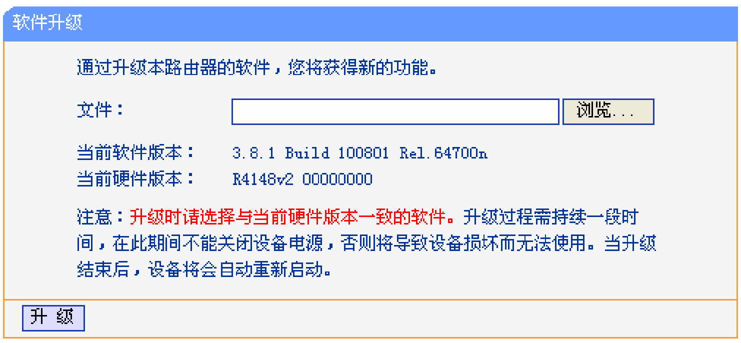
选择系统工具下的诊断工具，可以进入下面的诊断界面。使用 Ping 或者 Tracert 命令，可以诊断路由器的连接状态，页面如下：



- 选择端口　　　　选择需检测的端口。
- 选择操作　　　　选择 Ping 或者 Tracert 操作。
- IP 地址/域名　　目的 IP 地址或者域名。
- Ping 包数目　　Ping 操作发出的 Ping 包数目。
- Ping 包大小　　Ping 操作发出的 Ping 包的大小。
- Ping 超时设置　Ping 操作的超时时间。
- Tracert 跳数　　设置 Tracert 的跳数。

5.14.3　软件升级

选择系统工具下的软件升级，可以进入下面的软件升级界面。通过升级本路由器的最新版本软件获得最新的功能。升级页面如下：



举例:

升级步骤:

请先登录本公司的网站(www.tp-link.com.cn)，下载最新版本的软件。

选择系统工具下的软件升级项，在上图界面中的文件栏内填入已下载文件的全路径文件名，或用浏览按钮选择已下载的升级文件。

单击升级按钮进行软件升级。

升级完成后，路由器将自动重启。

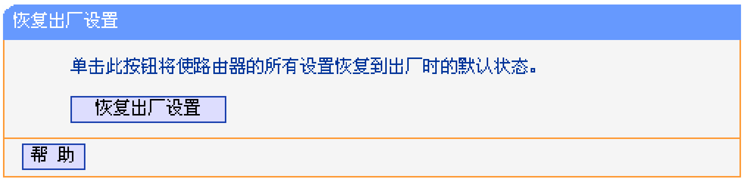
注意:

升级时请选择与当前硬件版本一致的软件。

在升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级过程需要一段时间，升级完成后，路由器将会自动重启。

5.14.4 恢复出厂设置

选择系统工具下的恢复出厂设置，可以进入下面的操作界面。单击恢复出厂设置按钮将使路由器的所有设置恢复到出厂时的默认状态。操作页面如下：



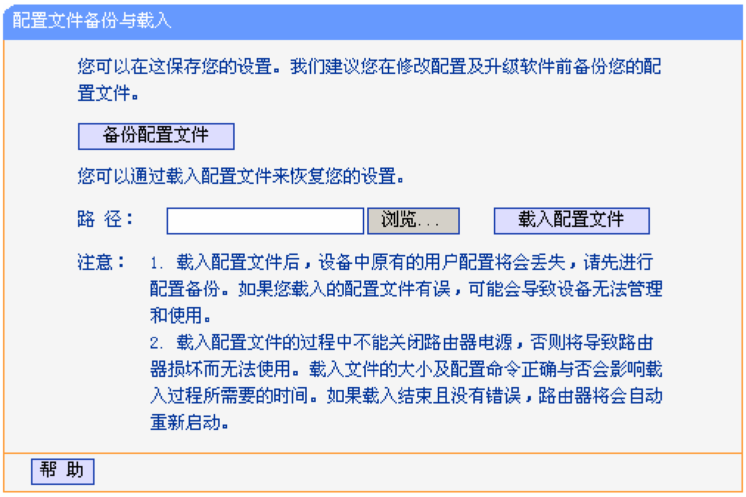
出厂默认情况下的各参数如下：

- 默认的用户名　admin
- 默认的密码　admin
- 默认的 IP 地址　192.168.1.1
- 默认的子网掩码　255.255.255.0

恢复出厂设置后，路由器将自动重启。

5.14.5 备份和载入配置

选择系统工具下的备份和载入配置，可以进入下面的操作界面。配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；配置载入功能则是将先前保存的或已编辑好的配置重新装入。配置界面如下：



- **备份配置文件**　　将配置以文件形式保存。
- **路径**　　配置文件的全路径。
- **浏览**　　选择配置文件。
- **载入配置文件**　　装入先前保存的或已编辑好的配置文件。

举例:

典型用法:

升级软件或在载入新配置文件前备份原配置，以防止升级软件或载入新配置文件时操作有误，丢失配置。

为多台路由器配置相同的设置。先设置一台路由器，保存其配置文件后，再将它载入到其它的路由器中，以节省时间。

注意:

载入配置文件后，设备中原有的用户配置将会丢失，如果您需要保存原有配置，请先进行配置备份。如果您载入的配置文件有误，可能会导致设备无法管理和使用。

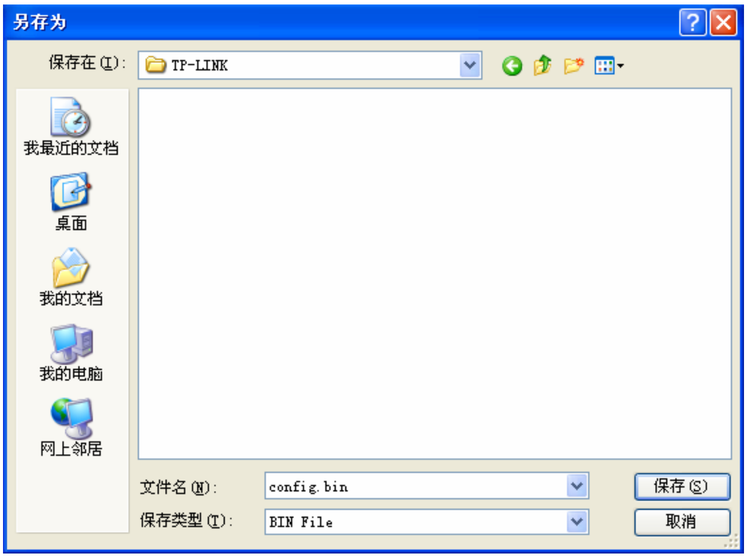
载入配置文件的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重启。如果载入有错，请根据提示信息及生效的配置选择自己是否需要保存配置，然后最好再重启路由器。

备份配置到：C:\TP-LINK\ config.bin；然后，将其载入到另一台路由器中。

备份配置步骤如下:

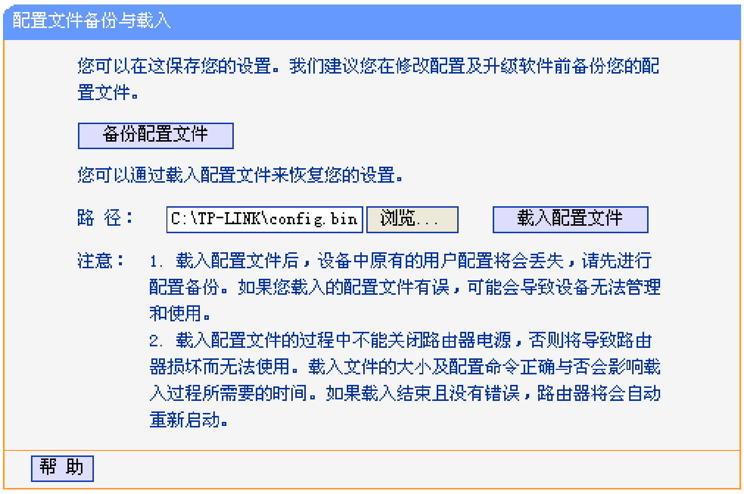
选择系统工具下的备份和载入配置项，单击备份配置文件按钮，出现下面操作界面:

点击保存按钮，将配置文件 config.bin 保存在文件夹 C:\TP-LINK 中。如下图示:



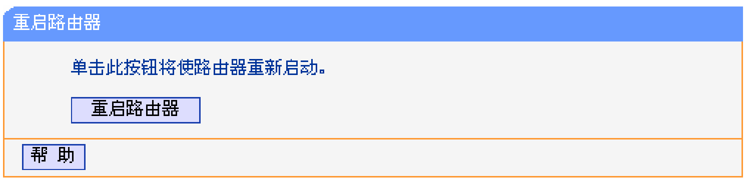
载入配置步骤如下:

更换另一台路由器，选择系统工具下的备份和载入配置项，输入载入文件夹的详细路径（如: C:\TP-LINK\config.bin）或点击浏览按钮选择载入文件夹，然后单击载入配置文件按钮即可完成文件载入。下图为输入文件路径，载入配置文件的示意图。



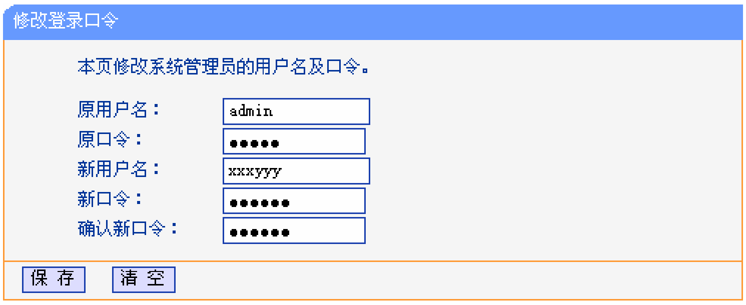
5.14.6 重启路由器

选择系统工具下的重启路由器，可以进入下面的操作界面。单击重启路由器按钮，路由器就会重新启动。操作界面显示如下：



5.14.7 修改登录口令

选择系统工具下的修改登录口令，可以进入下面的操作界面。本页修改系统管理员的用户名及口令。修改界面如下：



举例:

登录口令修改步骤:

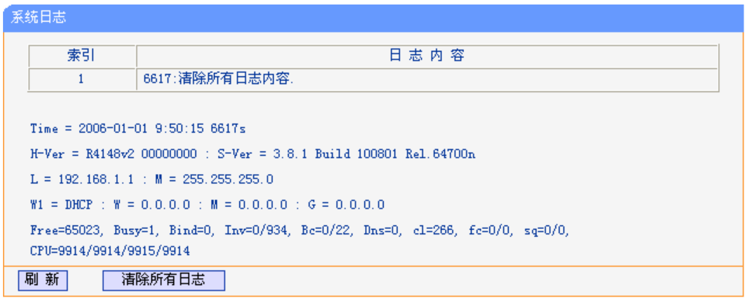
首先请您输入原来的用户名和口令，然后输入您希望使用的新用户名和口令。如果您原来的用户名和口令输入无误的话，单击“保存”即可成功修改用户名和口令。

注意:

出于安全考虑，我们强烈推荐您改变初始系统管理员用户名及密码。如果您忘了系统密码，请使用复位按钮恢复到出厂设置。

5.14.8 系统日志

选择系统工具下的系统日志，可以进入下面的显示界面。该部分记录了路由器的系统日志，您可以通过查询日志了解路由器上发生的系统事件。界面显示如下：



5.14.9 Syslog设置

选择系统工具下的 Syslog 设置，可以进入下面的操作界面。本页面设置 Syslog 服务。

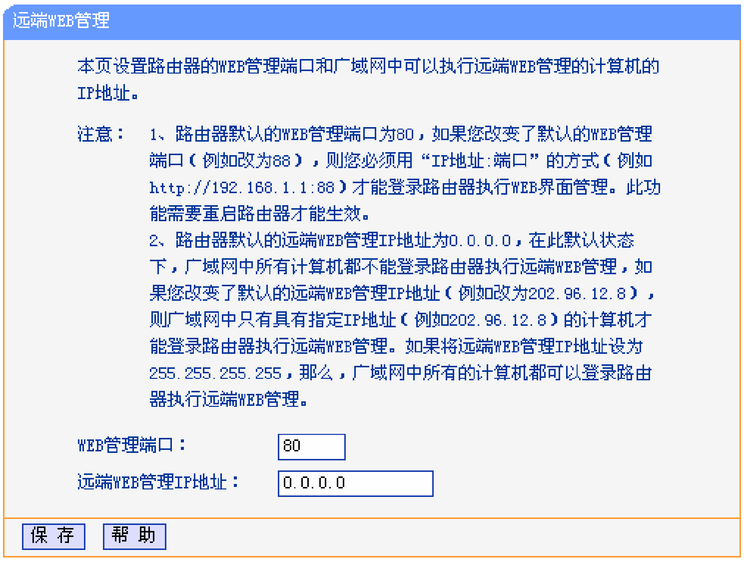


➢ **启用 Syslog** 请选择是否启用 Syslog 服务功能。

- **Syslog 服务器**　显示 Syslog 服务器的信息。
- 启用　请选择是否启用该 Syslog 服务器。
- 主机 IP 地址　请输入 Syslog 服务器的 IP 地址。
- 端口　请输入 Syslog 服务的协议端口（缺省端口为 514），可根据 Syslog 服务器设定的端口，进行修改；它应与 Syslog 服务器保持一致。

5.14.10 远端WEB管理

选择系统工具下的远端 WEB 管理，您可以进入下面的操作界面。本页设置路由器的 WEB 管理端口和广域网中可以执行远端 WEB 管理的计算机的 IP 地址。设置界面如下：



- **WEB 管理端口**　可以执行 WEB 管理的端口号。
- **远端 WEB 管理 IP 地址**　广域网中可以执行远端 WEB 管理的计算机的 IP 地址。

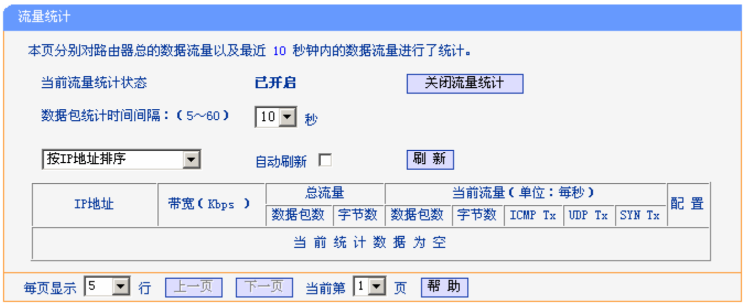
⚠ **注意:**

路由器默认的 WEB 管理端口为 80，如果您改变了默认的 WEB 管理端口(例如改为 88)，则您必须用“IP 地址端口”的方式（例如 http://192.168.1.1:88）才能登录路由器执行 WEB 界面管理。此功能需要重启路由器才生效。

路由器默认的远端 WEB 管理 IP 地址为 0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端 WEB 管理，如果您改变了默认的远端 WEB 管理 IP 地址（例如改为 202.96.12.8），则广域网中只有具有指定 IP 地址（例如 202.96.12.8）的计算机才能登录路由器执行远端 WEB 管理。

5.14.11 流量统计

选择系统工具下的流量统计，可以进入下面的操作界面。



- **当前流量统计状态**　　请您选择是否需要开启流量统计，如无需进行流量统计，可点击关闭流量统计按钮禁用该功能，这样可以提高路由器的数据处理能力。
- **数据包统计时间间隔**　　请您选择当前统计流量的时间间隔。它与“安全设置”－“高级安全设置”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。
- **流量统计列表**　　显示流量统计的信息。
- IP 地址　　显示被统计主机的 IP 地址。
- 带宽　　显示被统计主机 10 秒钟内收、发数据的字节数。
- 总流量　　显示当前数据的总流量，分别用数据包和字节数来衡量该值。
- 数据包数　　路由器总的收、发数据包的个数。
- 字节数　　路由器收、发数据的总计字节数。
- **当前流量**　　显示当前设置的时间间隔内（图中为 10 秒）的数据流量。
- 数据包数　　路由器当前 10 秒钟内收、发数据包的个数。
- 字节数　　路由器当前 10 秒钟内收、发数据的字节数。
- **ICMP Tx**　　路由器当前 10 秒钟内发送到广域网的 ICMP 包的个数。
- **UDP Tx**　　路由器当前 10 秒钟内发送到广域网的 UDP 包的个数。
- **TCP SYN Tx**　　路由器当前 10 秒钟内发送到广域网的 TCP SYN 包的个数。
- 每页显示　　设置每页可以显示的最大条目数（默认值为 5）。
- 上一页、下一页　　单击该按钮，可以分别转入界面的上一页或下一页。
- 当前第 页　　显示当前的页码。

5.14.12 IP地址转换表

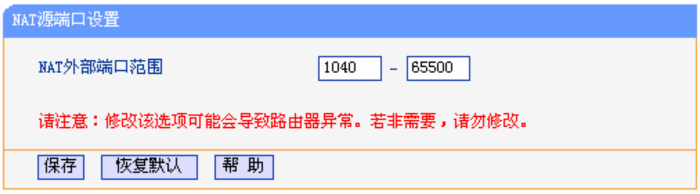
选择系统工具下的 IP 地址转换表，可以查看当前路由器的 IP 地址转换信息。当发生 IP 地址转换时，转换信息会自动添加进显示列表中，页面如下：



- 出口线路　　连接使用的路由器 WAN 口值。
- 协议类型　　连接使用的协议类型。
- IP 地址　　要查看连接的本地或远端主机的 IP 地址。
- 协议类型　　连接使用的协议类型。
- 本地 IP 地址　　LAN 端主机的 IP 地址。
- 本地端口　　该连接中 LAN 端主机使用的端口。
- 转换端口　　数据包经过 NAT 之后,WAN 口发出的数据包的源端口。
- 远端 IP 地址　　WAN 端主机的 IP 地址。
- 远端端口　　该连接中 WAN 端主机使用的端口。
- 老化时间　　表示该连接能够维持的时间(单位：秒)。
- 出口线路　　表示该连接使用的路由器 WAN 口号。

5.14.13 NAT源端口设置

选择系统工具下的 NAT 源端口设置，可以设置 NAT 外部端口范围。页面如下：



- NAT 外部端口范围　　设置数据包经过 NAT 地址转换后的外部地址的端口范围。默认值为 1040-65500。

5.14.14 证书设置

选择系统工具下的证书设置，您可以进入如下页面。

本路由器支持通过 HTTPS 方式进行配置。假设路由器 LAN 口的 IP 地址是 192.168.1.1，您就可以通过在浏览器地址栏中输入 https://192.168.1.1 进入配置页面，这时您与路由器之间的配置交互信息都是通过默认的安全证书加密的，大大提高了路由器的安全性。本页面可以根据您填的基本信息生成一个新的证书。



- 证书公共名称　　用户可输入自己定义的证书中的公共名称，此名称会在生成的新证书中出现。

➢ **电子邮件地址**　　用户可输入 E-Mail 地址，这个地址会在生成的新证书中出现。

⚠ **注意：**

1. 生成的新证书在重新启动路由器后才能生效。

2. HTTPS 方式暂不支持软件升级、配置文件载入等操作，如需进行此类操作请使用 HTTP 方式。

附录A FAQ

一. ADSL 用户如何设置上网？

1） 首先，将 ADSL modem 设置为桥模式（1483 桥模式）。

2） 用网线将路由器的 WAN 口与 ADSL modem 相连，电话线连 ADSL modem 的 Line 口。

3） 进入管理界面，选择菜单“网络参数”下的“WAN 口设置”，在右边主窗口中，“WAN 口连接类型”选择“PPPoE”，输入“上网帐号”及“上网口令”，点击连接按钮即可。

4） 如果是包月上网的用户，可以选择“自动连接”的连接模式；如果是非包月用户，可以选择“按需连接”或者“手动连接”，并且输入自动断线等待时间，防止忘记断线而浪费上网时间。

二. LAN 接入的用户如何设置上网？

1） 进入管理界面，选择菜单“网络参数”下的“WAN 口设置”，在右边主窗口中，“WAN 口连接类型”选择“动态 IP”，点击“保存”按钮即可。

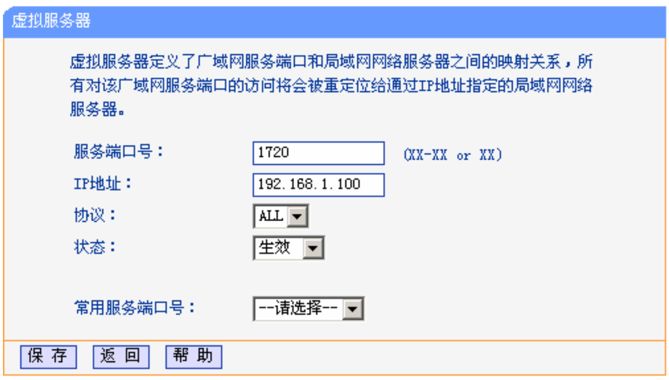
2） 在某些网络服务商绑定了用户计算机网卡 MAC 地址的情况下，需要对路由器进行 MAC 地址克隆操作，将路由器的指定 WAN 口（WAN1、WAN2、WAN3、WAN4）MAC 地址设置为被绑定的网卡 MAC 地址。选择菜单“网络参数”下的“MAC 地址克隆”，在右边主窗口中点击“克隆 MAC 地址”按钮，然后按“保存”按钮，待路由器重启动后生效。

三. 怎样使用 NetMeeting 聊天？

1） 如果是主动发起 NetMeeting 连接，则不需要任何配置，直接在 NetMeeting 界面中输入对方的 IP 地址，即可进行 NetMeeting 呼叫。

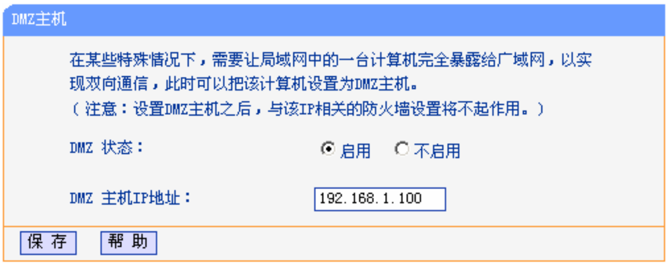
2） 如果希望能接收来自对方的 NetMeeting 呼叫，则需要设置虚拟服务器或 DMZ 主机。

3） 设置虚拟服务器方法：进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“1720”（NetMeeting 的连接端口），“IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.100），再在状态栏选择“生效”，点击“保存”按钮即可。如图：



这样，对方呼叫您时只需输入您路由器 WAN 口的地址即可。

4） 设置 DMZ 主机方法：进入管理界面，选择菜单“转发规则”下的“DMZ 主机”，在“DMZ 主机 IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.100），再将“启用”选择框选中，点击“保存”按钮即可。如图：

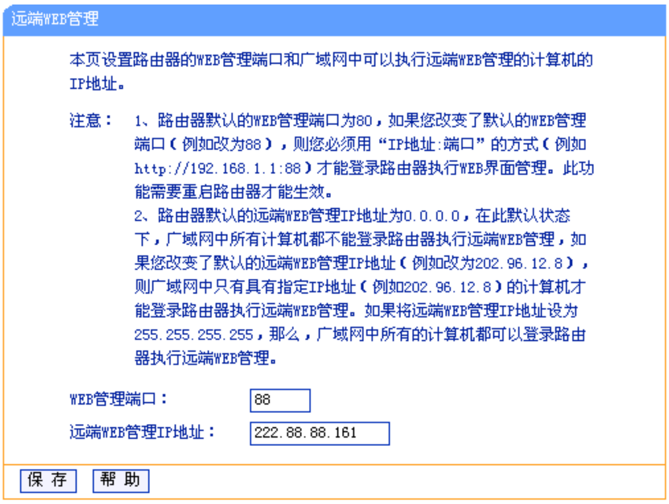


四. 怎样在局域网构建 Web 服务器？

1） 在局域网构建服务器，只需要按问题 3 的第三点设置虚拟服务器即可。

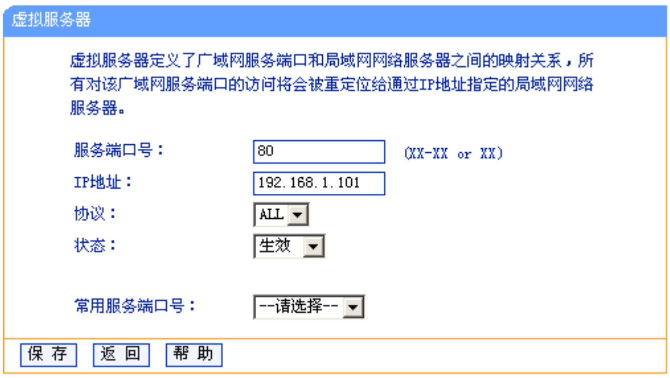
2） 但在构建 Web 服务器时，Web 服务的服务端口与路由器本身 Web 管理界面的缺省端口相同，都是 80，这样就引起冲突。解决办法是修改路由器 Web 管理界面的端口。

3） 进入管理界面，选择菜单“系统工具”下的“远端 Web 管理”，在右边主窗口中，“Web 管理端口”栏输入 80 以外的值，如 88。点击保存并重启路由器。如图：



4） 再次进入管理界面时，需要在浏览器的地址栏输入：http://192.168.1.1:88 才能进入。

5） 进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“80”，这是 Web 服务器的连接端口，“IP 地址”栏填入 Web 服务器的 IP 地址（假设您的 Web 服务器的 IP 地址是 192.168.1.101），再在状态栏选择“生效”，点击“保存”按钮即可。如图：



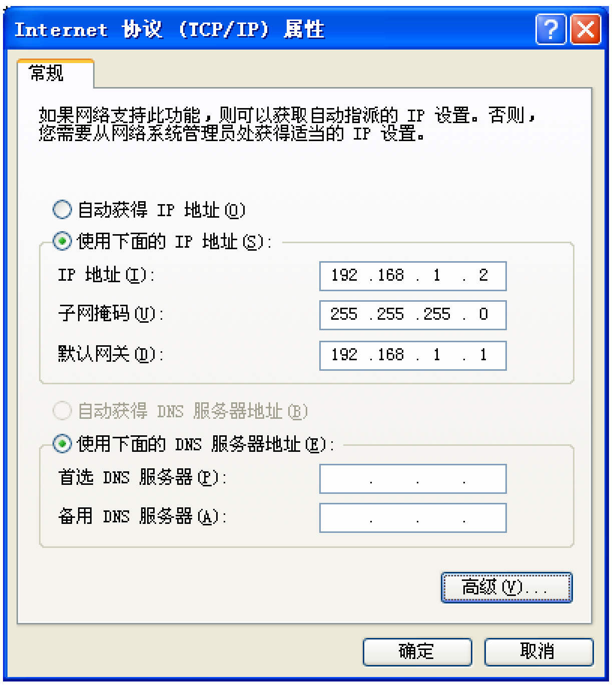
附录B　TCP/IP的详细设置

在这一节中将详细介绍 TCP/IP 的配置(本部分内容以 Windows XP 为例)：

1. 打开"开始→控制面板"中的"网络连接"，右键点击"本地连接"图标，单击"属性"选项，出现如下图所示页面：



2. 双击"Internet 协议"（TCP/IP），出现如下图所示页面。如果您希望拥有固定的 IP 地址，请选择**使用下面的 IP 地址**和**使用下面的 DNS 服务器地址**，然后手动设置网络参数，其中 IP 地址为 192.168.1.2－192.168.1.254 范围内的任意值，参数设置可以参照下图设置：



3. 如果您希望自动从路由器获得 IP 地址，请选择自动获得 IP 地址和自动获得 DNS 服务器地址，点击确定后设置将生效。

附录C　技术参数表格

<table>
<tr><td colspan="2">支持的标准和协议</td><td>IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS</td></tr>
<tr><td rowspan="3">端口</td><td>LAN口</td><td>4个10/100M自适应RJ45端口（Auto MDI/MDIX）</td></tr>
<tr><td>WAN口</td><td>1个10/100M自适应RJ45端口（Auto MDI/MDIX）</td></tr>
<tr><td>其它</td><td>1个Console端口（RJ45）</td></tr>
<tr><td colspan="2" rowspan="2">网络介质</td><td>10Base-T：3类或3类以上UTP</td></tr>
<tr><td>100Base-TX：5类UTP</td></tr>
<tr><td rowspan="2">LED指示灯</td><td>LAN/WAN口</td><td>Link/Act（连接/工作）、100Mbps（速率）</td></tr>
<tr><td>其它</td><td>PWR（电源）、SYS（系统状态）</td></tr>
<tr><td colspan="2">外形尺寸(L x W x H)</td><td>294mm x 180mm x 44mm</td></tr>
<tr><td colspan="2" rowspan="4">使用环境</td><td>工作温度：0ºC~40ºC</td></tr>
<tr><td>存储温度：-40ºC~70ºC</td></tr>
<tr><td>工作湿度：10%~90%RH 不凝结</td></tr>
<tr><td>存储湿度：5%~90%RH 不凝结</td></tr>
<tr><td colspan="2">电源输入</td><td>100-240V~ 50/60Hz 0.3A</td></tr>
</table>

深圳市普联技术有限公司
TP-LINK TECHNOLOGIES CO., LTD.
技术支持热线：400-8863-400
公司地址：深圳市南山区桃源街道平山大园工业区南区2栋1-6楼
技术支持E-mail：smb@tp-link.com.cn
http://www.tp-link.com.cn